

Final Report

GENERIC HEALTH MANAGEMENT

A

SYSTEM ENGINEERING PROCESS

HANDBOOK

OVERVIEW AND PROCESSES

FINAL REPORT

REF: CONTRACT NO. NAS8-40365

DECEMBER 15, 1995

Submitted to:
Systems Requirements & Verification Branch
Systems Engineering Division
Systems Analysis and Integration Laboratory
George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama 35812

ALPHA TECHNOLOGY

3322 S. MEMORIAL PARKWAY, SUITE 215H, HUNTSVILLE, AL 35801

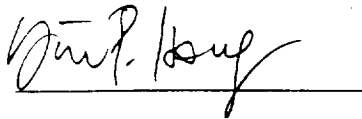
GENERIC HEALTH MANAGEMENT
A
SYSTEM ENGINEERING PROCESS
HANDBOOK
OVERVIEW AND PROCESSES

REF. CONTRACT NO. NAS8-40365

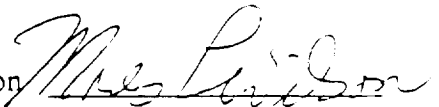
DECEMBER 15, 1995

Submitted to:
Systems Requirements & Verification Branch
Systems Engineering Division
Systems Analysis and Integration Laboratory
George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama 35812

Yin Paw Hong
President



Moses L. Wilson
Principle Investigator



ALPHA TECHNOLOGY
3322 S. MEMORIAL PARKWAY, SUITE 215H, HUNTSVILLE, AL 35801

TABLE OF CONTENTS

I.0 INTRODUCTION	1
I.1 BACKGROUND	1
I.2 APPROACH	2
I.3 GOALS	7
II.0 PURPOSE.....	8
III.0 SCOPE	9
IV.0 DESCRIPTION.....	11
IV.1 NARRATIVE (OVERVIEW).....	11
V.1.1 THE INITIAL REQUIREMENTS PHASE.....	11
IV.1.1.1 COST EFFECTIVENESS AND RELIABILITY/RISK ANALYSIS	16
IV.1.2 CONCEPTUAL DESIGN PHASE	19
IV.1.2.1 REQUIREMENTS (GENERAL AND TYPICAL-CANDIDATES)	21
IV.1.3 THE PRELIMINARY DESIGN PHASE.....	24
IV.1.4 THE DETAIL DESIGN PHASE	28
IV.1.5 FAB AND TEST PHASE	30
IV.1.6 OPERATIONS PHASE	30
V.0 METHODOLOGY.....	31
V.1 DECISION MAKING PROCESS	31
V.2 HEALTH MANAGEMENT MEASUREMENT PROGRAM DEVELOPMENT PROCESS	32
V.3 FF-DAREL DEVELOPMENT PROCESS	36
V.4 INTER-SYSTEM INFORMATION RELATIONSHIP LISTING (ISIRL) DEVELOPMENT PROCESS.....	44
V.5 HM REQUIREMENTS GENERATION.....	47

LIST OF FIGURES

FIGURE III-1 TYPICAL PROGRAM PHASING WITH HEALTH MANAGEMENT	10
FIGURE IV-1A HEALTH MANAGEMENT FLOW	12
FIGURE IV-1B HEALTH MANAGEMENT FLOW	13
FIGURE IV-2 DESIGN CHARACTERISTICS CORRELATION MATRIX	15
FIGURE IV-3 COST EFFECTIVENESS EXAMPLE	18
FIGURE IV-4 HEALTH MANAGEMENT IMPLEMENTATION LEVEL DECISION	27
FIGURE V-1 HEALTH MANAGEMENT MEASUREMENT PROGRAM (HM-MP) FORMAT	35
FIGURE V-2 HM-MP PROCESS FLOW	36
FIGURE V-3 TYPICAL FUNCTIONAL FAILURES	39
FIGURE V-4 TYPICAL FUNCTIONAL FAILURE CAUSES	39
FIGURE V-5 FF-DAREL WORKSHEET	42
FIGURE V-6 ISIRL SYSTEM	46
FIGURE V-7 HEALTH MANAGEMENT SYSTEM ENGINEERING PROCESS	51

LIST OF TABLES

TABLE I-1 INTEGRATED SYSTEM ENGINEERING PROCESSES WITH TIME-RELATED HEALTH MANAGEMENT PROCESSES	3
TABLE I-2 SYSTEMS ENGINEERING AREAS OF EXPERTISE	6

LIST OF APPENDICES

APPENDIX I HEALTH MANAGEMENT PROCESSES TO EXISTING SECTIONS OF SYSTEM ENGINEERING HANDBOOK	52
APPENDIX II MATRIX HM SUBJECT TO REFERENCE DOCUMENT	53
APPENDIX III.1 STATE OF THE ART HEALTH MONITORING TECHNIQUES ON BOARD NAVAL VESSELS	54
APPENDIX III.2 NEURAL NETWORK APPROACH TO SPACE SHUTTLE MAIN ENGINE HEALTH MONITORING	58
APPENDIX III.3 HEALTH MONITORING SYSTEM FOR THE SSME HARDWARE ARCHITECTURE STUDY	60
APPENDIX IV DEFINITIONS	62

LIST OF REFERENCED DOCUMENTS

Contains the listing of documents that are referenced in this final report and some additional documents of value to the customer. The latest issue of each document is applicable

- 1 Rocket Engine Condition Monitoring System (RECMS) Final Report SHM Design Methodology, Martin Marietta, Space Launch Systems Company, Denver, Colorado. 30 October 1992
- 2 NASA Reference Publication 1358, System Engineering "Toolbox" for Design-Oriented Engineers, Goldberg-Everhart-Stevenson-Babbitt-Clemens-Strout, Marshall Space Flight Center, Alabama, December 1994
- 3 AIAA-90-1993, Rocket Engine Failure Detection Using System Identification Techniques, C.M. Meyer & J.F. Zakrajsek, Sverdrup Technology, Inc., July 16-18, 1990
- 4 Improving Systems Monitoring and Failure Detection/Prediction on Future Spacelab Missions, Final Report, Purchase Order H18767D, Alpha Technology, March 10, 1993
- 5 AIAA-90-2697, Integrated Health Monitoring Approaches and Concepts for Expendable and Reusable Space Launch Vehicles, J.G. Johnson - General Dynamics Space Systems Division, San Diego, California, July 16-18, 1990
- 6 Systems Engineering Management Guide, U.S. Government Printing Office, January 1990
- 7 Vehicle Health Monitoring System Study (VHMSS), Final Report, D18032235-1, AL-TR-90-074, Boeing Defense and Space Group, Seattle, Washington, October 1990
- 8 Orbit Transfer Rocket Engine Technology Program-Integrated Controls and Health Monitoring Fiber-Optic Shaft Monitor, Final Report, RI/RD 90-177, Rocketdyne Division of Rockwell International Corp., Canoga Park, California, November 1989
- 9 Real Time Fault Monitoring of Industrial Processes, A. D. Pouliezos and G. S. Stavrakakis Kluwer Academic Publishers, Norwell, Massachusetts, 1994
- 10 NASA Systems Engineering Handbook, Robert Shishko, SP-6105, June 1995
- 11 Engineering Design for Producibility and Reliability, John W. Priest, Marcel Dekker, Inc., New York, New York, 1988

LIST OF REFERENCED DOCUMENTS (Cont)

- 12 System Engineering Handbook, Vol 1 & Vol 2, MSFC-HDBK-1912A, December 6, 1994

MSFC-HDBK-1912A System Engineering Handbook, Volume 1 - Overview and Processes, December 6, 1994

MSFC-HDBK-1912A System Engineering Handbook, Volume 2 - Tools, Techniques, and Lessons Learned, December 6, 1994
- 13 AIAA-90-2259, Neural Network Approach to Space Shuttle Main Engine Health Monitoring - B Whitehead, H. Ferber, M. Ali - UTSI, Tullahoma, Tennessee, July 16-18, 1990
- 14 AIAA-90-1991, Development of a Health Monitoring Algorithm - E. Nemeth and A M Norman, Jr., Rockwell International/Rocketdyne Division, Canoga Park, California, July 16-18, 1990
- 15 AIAA-90-1990, Multi-Sensor Analysis Techniques for SSME Safety Monitoring - W A Maul - Sverdrup Technology, Inc., Brook Park, Ohio, July 18, 1990
- 16 AIAA-90-1988, Health Monitoring System for the SSME-Failure Detection Algorithms - S Tulpule and W S Galinaitis, United Technologies Research Center, East Hartford, Connecticut, July 16-18, 1990
- 17 AIAA-90-1987, Health Monitoring System for SSME - Program Overview-M W Hawman- United Technologies Research Center, East Hartford, Connecticut, July 16-18, 1990
- 18 Problem Solving Seminars in "----- Simulation, Forecasting, Expert Systems The Institute for Professional Education, Arlington, Virginia. (September 1995-June 1996)
- 19 MSFC-STD-1924, Standard for Instrumentation Program And Control Lists (IP&CL), June 21, 1993
- 20 State-of-the-Art Health Monitoring Techniques Onboard Naval Vessels, TNO Building and Construction Research, TNO Report 94-CMC-R1037, August 25, 1994
- 21 ASAT Mission and System Effectiveness Partial Report
- 22 Health Management Cost/Benefit, Jeffrey H. Albert, The Boeing Company, December 11-12, 1990

LIST OF REFERENCED DOCUMENTS (Cont)

- 23 Neural Networks Analyze Data in "Particle-Impact-Noise Detection Test" (PIND), Lewis Research Center, Cleveland, Ohio, NASA Tech Briefs, October 1995
- 24 Algorithm Helps Monitor Engine Operation, Eckerlin, Pannossian, Kemp, Taniguchi, Nelson - Rockwell International for MSFC, Huntsville, Alabama, NASA Tech Briefs, November 1995
- 25 Requirements for Preparation and Approval of Failure Modes and Effect Analysis (FMEA) and Critical Items List (CIL), NSTS 22206, Rev D, December 10, 1993
- 26 Built-In-Diagnosis (BID) of Equipment/Systems, Granieri, Giordano, Nolan (Giordano Automation) For McDonnell Douglas/MSFC, MSFC, Alabama, NASA Tech Briefs, December 1995
- 27 Merriam-Websters Word-Watch, Springfield, Massachusetts - November 1995
- 28 A System Health Management Design Methodology, Puening, Martin Marietta Astronautics Group, Denver, Colorado, November 17-18, 1992
- 29 SAE-921031, Integrated Health Monitoring and Controls for Rocket Engines- W C Merrill, J L. Musgrave, and T.H.Guo - NASA Lewis Research Center, Tech Paper, SAE Aerospace Atlantic, Dayton, Ohio, April 7-10, 1992
- 30 Research and Technology Goals and Objectives for Integrated Vehicle Health Management (IVHM), OAST, NASA HQ, Washington, D C., October 10, 1992
- 31 SAE-921007, Health Monitoring of Reusable Rocket Engines-W. Ezell, S. Barkhoudarian and G Cross (Rockwell International) Tech Paper, SAE Aerospace Atlantic Dayton, Ohio, April 7-10, 1992
- 32 AIAA-90-3540, Space Station Transition Through Spacelab, H Craft, NASA-MSFC, Huntsville, Alabama, September 25-28, 1990
- 33 AIAA-89-2755, Smart Sensor Technology for Advanced Launch Vehicles-J Schoess, Honeywell Systems and Research Center, Minneapolis, Minnesota, July 10-12, 1989
- 34 AIAA92-1477, Vehicle Health Management Technology Needs, W E. Hammond & W G Jones, Sverdrup Technology Inc., MSFC, Alabama, March 24-27, 1992
- 35 Vehicle Health Management Technology Briefing-Panel Meeting - J. Schoess, G Hadden, Honeywell Systems and Research Center, November 16, 1992

LIST OF REFERENCED DOCUMENTS (Cont)

- 36 Reliability Evaluation of Engineering Systems Concepts and Techniques, Roy Billinton & Ronald N. Allan, Plenum Press, New York, New York 1992
- 37 Logistics Engineering and Management, Fourth Edition, Benjamin S. Blanchard, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1992
- 38 Systems Engineering and Analysis, Second Edition, Benjamin S. Blanchard & Walter J. Fabrycky, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1990

LIST OF ACRONYMS AND ABBREVIATIONS

ADAM	Aural Definition with ANN Modeling
ADIR	Aural Definition of Intersystem Relationships
ADIRMA	Aural Definition of Intersystem Relationships with Modeling Assistance
ANN	Artificial Neural Network
ASAT	Anti-Satellite
B/L	Baselined
BIT	Built-In-Test
BITE	Built-In-Test-Equipment
C E	Cost Effectiveness
CCB	Configuration Control Board
CDR	Critical Design Review
CIL	Critical Items List
DDE	Detail Design Engineer
DIP	Diagnostic Information Processing
DOC	Document
DR	Documentation Requirement
FF-DAREL	Functional Failure-Definition and Resulting Effects Listing
FMEA	Failure Modes and Effects Analysis
FRR	Flight Readiness Review
GSE	Ground Support Equipment
HDBK	Handbook
HM	Health Management
HM-MP	Health Management Measurement Program
HW	Hardware
IP&CL	Instrumentation Program and Command List
ICMOS	Intelligent Control and Monitoring System
ISIRL	Inter-System Information Relationship Listing
LRU	Line Replaceable Unit
MSFC	Marshall Space Flight Center
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NASA	National Aeronautics and Space Administration

LIST OF ACRONYMS AND ABBREVIATIONS (Cont)

NSTS	National Space Transportation System
PDR	Preliminary Design Review
PMS	Probability of Mission Success
PI	Principle Investigator
RECMS	Rocket Engine Condition Monitoring System
REF	Reference
RLV	Reusable Launch Vehicle
S&E	Science and Engineering
S&MA	Safety and Mission Assurance
SAR	System Acceptance Review
SW	Software
S E	System Effectiveness
SE	System Engineer
SRD	System Requirements Document
SRR	System Requirements Review
SSME	Space Shuttle Main Engine
STS	Space Transportation System
TPS	Thermal Protection System
VHM	Vehicle Health Management
VRSD	Verification Requirements and Specification Document

I.0 INTRODUCTION

I.1 BACKGROUND

This document is being prepared as an extension of the concepts and approaches defined in the limited initial study "Improving Systems Monitoring and Fault Detection/Prediction on Future Spacelab Missions" (Reference 4. Document). The depth of penetration and detail will be expanded and upgraded as approaches and techniques are developed and defined which are necessary for implementing Health Management on future Spacelab/Space Station type Payloads, Space Transportation System (STS) Enhancements, New Launch Vehicles, such as Reusable Launch Vehicle (RLV), and other Space Systems.

Health Management, a System Engineering Process, is defined as "Those processes-techniques-and-technologies used to define, design, analyze, build, verify, and operate a system from the viewpoint of preventing, or minimizing, the effects of failure or degradation." It supports all ground and flight elements during manufacturing, refurbishment, integration, and operation through combined use of hardware, software, and personnel.

The "Integrated Diagnostic Concept", focused as End-to-End Information Management, and suggested as being implemented by Diagnostic Information Processing (DIP) in the initial study, is expanded to delineate the necessary Plans, Requirements, Procedures, and Methodology for implementation. Highlights of the initial study will be reiterated and details provided which are sufficient for implementing various defined DEGREES of Health Management on applicable Aerospace Projects.

Complicating the Health Management effort are many factors:

- * Variable Design Teams (depending on size/complexity of project)
- * Skills and Specialities
- * System Complexity
- * Many different goals, requirements and agendas, not all especially concerned with Health Management (or they conceive it in a different or cursory manner, or with a different priority)

- * Task personnel (skilled Engineers) located in many areas, possibly widely separated and in different companies, or organizations, all responding to Project Managers who are determined to keep costs down and schedules intact, but demanding a high probability of project success

Efforts required to accomplish Health Management are highlighted in this Handbook, and a Matrix is included showing Phased-In Processes to existing Sections of the "System Engineering Handbook, MSFC-HDBK-1912A" if inclusion should be desired (See Appendix I) This Document, however, will be a Stand Alone entity

I.2 APPROACH

Health Management is defined in this Document as a Subprocess of the System Engineering Process. In reality, Health Management consists of many efforts, accomplished in each Phase of NASA's five Phased Project Steps, (See Figure III-1) but accomplished in conjunction with other standard System Engineering efforts. (See Table I-1, Integrated System Engineering Processes with Time-Related Health Management Processes) These processes, which are required throughout a project's Life Cycle, will be outlined, described and sequenced throughout the Five Phases. Early Health Management efforts are absolutely necessary if it is to be implemented on any project and they must be accomplished if it is to be effective. Like all System Engineering, Health Management must be dynamic, that is, it must evolve, when needed or desired, into accomplishing the results that any Project Engineer expects for that specific Project -- however, it must never be in the critical path of a project's development.

This document will integrate Health Management Processes [Six (6) HM Phases] into the Five (5) Project Phases in such a manner that it is never a stand alone task/effort which separately defines independent work functions. This division would create isolationism in design and planned usage and would never be effective in operations. So Systems Engineering personnel will coordinate the development and integration of all Requirements for System and Detail Design, Reliability, Maintainability, Safety, Survivability, and Health Management and other such efforts into the total Engineering effort, and will insure that all Requirements are identified and baselined

to meet the Project objectives during the Project Life Cycle. (Reference Table I-2, Systems Engineering Areas of Expertise)

TABLE I-1
INTEGRATED SYSTEM ENGINEERING PROCESSES
WITH TIME-RELATED HEALTH MANAGEMENT PROCESSES

SE--Standard System Engineering Processes

HM--Health Management Sub-Processes

Phase A

A-SE-1	Project Objectives
A-HM-1	Health Management Definition Statement and Generalized Intent
A-SE-2	Research and advanced technology requirements
A-HM-2	Process Improvement through Sensor/computer technology/software technology investigations -- Search for State-of-the-Art or newly developed tool-box advancements in Health Management technology-- Emphasize search for any deficient aspect
A-SE-3	Trade-off analysis
A-HM-3	Explore depths of potential Health Management implementation using Level I requirements (See Table IV-4, Health Management Implementation Level Decision)
A-SE-4	Selection of system concepts
A-HM-4	Inputs (options) to be included in risk/cost analysis (See Figure IV-3, Cost Effectiveness Example) and defined in Preliminary System Requirements and reflected in preliminary studies

Phase B

B-SE-1	Development of System Requirements Document (SRD) and Science and Engineering (S&E) Implementation Plan
B-HM-1	Define Health Management goals and develop Requirements for inclusion in SRD
B-SE-2	Refinement of selected alternative concepts and trade-off analysis
B-HM-2	Options derived/selected from Phase A to be explored with cost versus gain emphasized--Cost Effectiveness update

- B-SE-3 Perform trade-off analysis
- B-HM-3 Refine depth/cost trades of levels appropriate to project complexity and Level I requirements
- B-HM-4 Perform Preliminary Fault Tolerance Analysis

- B-SE-4 Refinement of system and support requirements
- B-HM-5 Develop Preliminary Versions of:
 - (a) Inter-System Information Relationship Listing (ISIRL)
 - (b) Health Management-Measurement Program (HM-MP), and
 - (c) Functional Failure-Definition and Resulting Effects Listing (FF-DAREL).

- B-HM-6 Drive out Health Management Requirements for Specific Projects utilizing the HM Requirements Generation Process described in Methodology Section V.5 of this Handbook

- B-HM-7 Develop Test Bed/Simulation Functional Fault Requirements

- B-HM-8 Baseline Health Management Requirements at System Requirement Review (SRR)

- B-SE-5 Definition of Preliminary Test Requirements
- B-HM-9 Identify Preliminary verification methods/requirements for verifying and utilizing ISIRL in test operations

- B-SE-6 Preliminary Design Review (PDR) baseline
- B-HM-10 Participate in Preliminary Design Review (PDR) with focus on implementation of baselined Requirements and ISIRL development

Phase C

- C-SE-1 Performance of detailed system analysis
- C-HM-1 Detailed analysis of Inter-System Information Relationship Listing (ISIRL) -- and Functional Failure-Definition and Resulting Effects Listing (FF-DAREL)

- C-HM-2 Perform detailed "Time To Criticality" Analysis of all identified Functional Failures

- C-HM-3 Perform Test Bed/Simulation Functional Faults

- C-SE-2 Completion of detail design
- C-HM-4 Establish methods of expressing the Inter-System Information Relationships (Both in software algorithms/statements and by manual procedure statements)

- C-SE-3 Develop final Manufacturing-Test-Verification-Integration- Operations supporting systems, facility plans, and VRSD
- C-HM-5 Develop criteria and finalize the degree/depth of Health Management being implemented--Insure its functions are included in all Plans, IP&CL, VRSD and other applicable documents. Update Cost Effectiveness Analysis
- C-SE-4 Perform Critical Design Review (CDR)
- C-HM-6 Finalize ISIRL, FF-DAREL and insure all Health Management Statements (Software and Manual) are documented in the ISIRL, including those functions operating behind the scene, those requiring operator decision/intervention, and either by crew or by ground operations. Finalize Plans and Requirements for Verification/Validation of all Statements via the VRSD.

Phase D

- D-SE-1 Development and test of prototype/protoflight hardware
- D-HM-1 Utilization of prototype/protoflight hardware to study effectiveness of implemented Health Management
- D-SE-2 Verification/validation-qualification of Hardware and Software for flight
- D-HM-2 Establish, through test, accurate/dependable/confident HealthManagement operations to degree being implemented
- D-SE-3 Manufacture, Integrate and Checkout flight systems
- D-HM-3 Satisfy all VRSD Requirements for implemented Health Management

Phase E

- E-SE-1 Support flight and evaluate functional operations
- E-HM-1 Support flight operations and evaluate Health Management functionality--determine effectiveness in terms of fault detection-prevention-recovery

This concept of Health Management (HM) must be accomplished through Panel/Working Groups focused on establishing Inter-System Relationships of Measurements and Information as discussed in the Description Section. The familiar facets of HM that address Availability, Reliability, and Maintainability (such as Line Replaceable Unit (LRU) physical replacement and spare availability) are not a significant element in this concept. The Process must be accomplished using the skills of System Engineers, Detail Designers, Safety & Mission Assurance (S&MA)

Personnel, Project Personnel, Software Designers, Test, Science and Mission Operations Personnel.

The Basic Theme is that there is an additional Level of Information which contains Multi-System data, which is necessary to make choices and decisions--but which is not often developed--but can be gleaned from the skills of the Engineering personnel listed above and by the described processes in this Handbook.

The Proactive Process of Planning for, anticipating, and developing the use of this Level of Information during all Life Cycle Phases is key to the success of Health Management as described in this Handbook.

Conceptual Layout	End-to-End Functional Schematics
Orbital and Flight Mechanics	System Design
Guidance and Navigation*	Interface Definition and Control
Electromagnetic Compatibility/Interference*	Lightning Protection
Resource Utilization Reporting (Mass Properties, Electrical Power, Instrumentation and Commands)	Ground Integration and Operations
System Verification Planning and Requirements Compliance	
Spacecraft Charging	GSE Requirements
Natural Environments (Space and and Terrestrial)	Systems Requirements
Health Management*	System Test/Verification

* = Added Area of Prime Expertise

TABLE I-2. SYSTEMS ENGINEERING AREAS OF EXPERTISE

I.3 GOALS

The Goals for Health Management implementation are as follows:

- * Allow the Project Manager to select an appropriate degree of Health Management suitable for that Project.
- * Health Management must "**ADD VALUE**" to a Project without increasing **Life Cycle** cost
- * No new Documentation Requirements (DR's) nor Reports are required
- * No new Technology is required to implement the various Degrees of this Health Management concept.
- * All Processes are to be fully described in Layman's Terms for better understanding and optimum implementation.
- * This Health Management effort is to be invisible to those who seek to find identifiable, dedicated manpower Level-of-Effort--It will be meshed in with other System Engineering effort and Design Tasks--but--it does have Identifiable Goals, Requirements, and Specific Methodologies.
- * This Document will be a stand-alone treatise on Health Management from a System Engineering viewpoint, providing definition of phased in Proactive Processes to be accomplished during Phased Project Development. It will be suitable for inclusion as an Applicable Document in a contracted project environment.

II.0 PURPOSE

As earlier stated, Health Management must be accomplished through organized effort. It will not happen if not focused, coordinated, and directed by strong System Engineering thrust. A mandate from the Project Manager must be given to support and develop the affordable and selected degree of Health Management to be implemented and it must not be fulfilled as a jerkwater task/process.

The concept and methodology described in this Handbook requires the use of skills and knowledge and key inputs of Subsystem, System, and Scientific Instrument detail designers and developers. System Engineers, together with these hardware designers, software designers, Project Engineers, Test, Safety and Mission Assurance, and Operations Personnel will accomplish the layout and implementation of sensors, fault controls (hardware and software), and effectors to detect, prevent, isolate, and recover from all potential faults that can be discerned by extensive analysis, investigation, or additionally determined by standard modeling practices, and by artificial neural network (ANN) prediction. Decisions can be made on dealing with, or treating, these discerned faults either in-flight, on the ground, and either by human decision/determination, or computer control and software logic--or by a combination of all these options. Typical Trade Studies, identified in this Handbook (See Section IV, DESCRIPTION, Initial Requirements Phase, Conceptual Design Phase, and Preliminary Design Phase), or which may be identified as needed during active Project development, will help select specific methods to detect, and deal with specific faults, impending faults, controls and recoveries. These efforts comprise the Health Management Process (Concept) described in this Handbook and are shown in the "Health Management Flow", Figure IV-1.

This Handbook provides the methods and identifies the design provisions to aid in both preventing the occurrence of faults and mitigating the effect of faults that do occur. This is accomplished by developing the additional level of multi-system Information (more than just measurements reflecting data, status, and scientific information) which is needed for making choices and decisions which have a significant impact on failure and/or successes of aerospace endeavors. Therefore, the overriding purpose of this Handbook is to describe the efforts/processes, and who performs these efforts, which are needed to be accomplished in all Life Cycle Phases in order to have effective Health Management.

III.0 SCOPE

Health Management, as it is applicable to Spacelab/Space Station Payloads, STS Enhancements, Reusable Launch Vehicles (RLV), or other Space Systems, i.e., Scientific Experiments, is more than "Health Monitoring"--First, it is an organized method, coordinated and directed by a strong System Engineer and secondly, it makes maximum and cooperative use of skills of Sub-System and Scientific Instrument Detail Designers. Although it is emphasized that no new technology is required, these processes make maximum use of existing skills and enhancing technology. It is recognized that new/advanced technology occurs every year. Enhancing Technology, more visible through Investigative and Trade Studies, as appropriate, is encouraged, especially in areas of sensors, smart devices, computer/control technology, and software advances and updated versions.

This Document describes the discipline of Health Management for "Systems" as used on vehicles, payloads and/or experiments. It consists of processes, techniques, and technologies used to design, analyze, build, verify, and operate that system from a viewpoint of preventing, or minimizing, the effects of failures. All Functional Faults, or failures, will be addressed and these are not addressed as Safety issues, but only as they may degrade planned operational behavior. This process will explicitly be based on "Information" generation, correlation, processing and feedback as defined in our Initial Study (Ref. 4) but now is expanded with strategy and considerations (steps/plans/studies) outlined for use in understanding and making use of three incremental degrees, or levels, which could be implemented. All efforts will be identified to the Life Cycle Phasing, although some shifting between phases, or sequencing, will probably be needed, or desired, on some projects. Accomplishing the efforts/processes in different development Phases than those recommended/identified in this Handbook can result in effective Health Management, but may not be as "Cost Effective" (See Section IV.1.1.1, Cost Effectiveness and Reliability/Risk Analysis).

The description of Efforts/Processes required in this Health Management approach and the Degrees of Implementation are discussed in Section IV.0 (Description) and are presented at a working level and in layman's terms since it is felt that the most effective paths are those which

can be readily understood and involve less complexity. This approach and description are also most important since Health Management, in all cases, can not be separated from Safety Issues and Paths because many functional faults trace, or propagate, into safety related paths. **We do not, however, intend to address safety issues, plans, nor processes/procedures** in this Handbook.

Functional Failure-Definitions and Resulting Effects Listing (FF-DAREL)

Worksheets will be developed and used by the System Engineer as a key element in this process. The FF-DAREL is an expanded FMEA which is developed over a different time frame and is only a Working Document which provides a means of identifying and managing all potential failures/faults. These Worksheets are discussed in more detail in Section V. (METHODOLOGY), and may be of benefit in FMEA/CIL development which normally occurs later in the Development Phases than these Worksheets.

Health Management is just one of many System Engineering Jobs--but it is not just a System Engineering Job, but requires effort/emphasis by **ALL DISCIPLINES**.

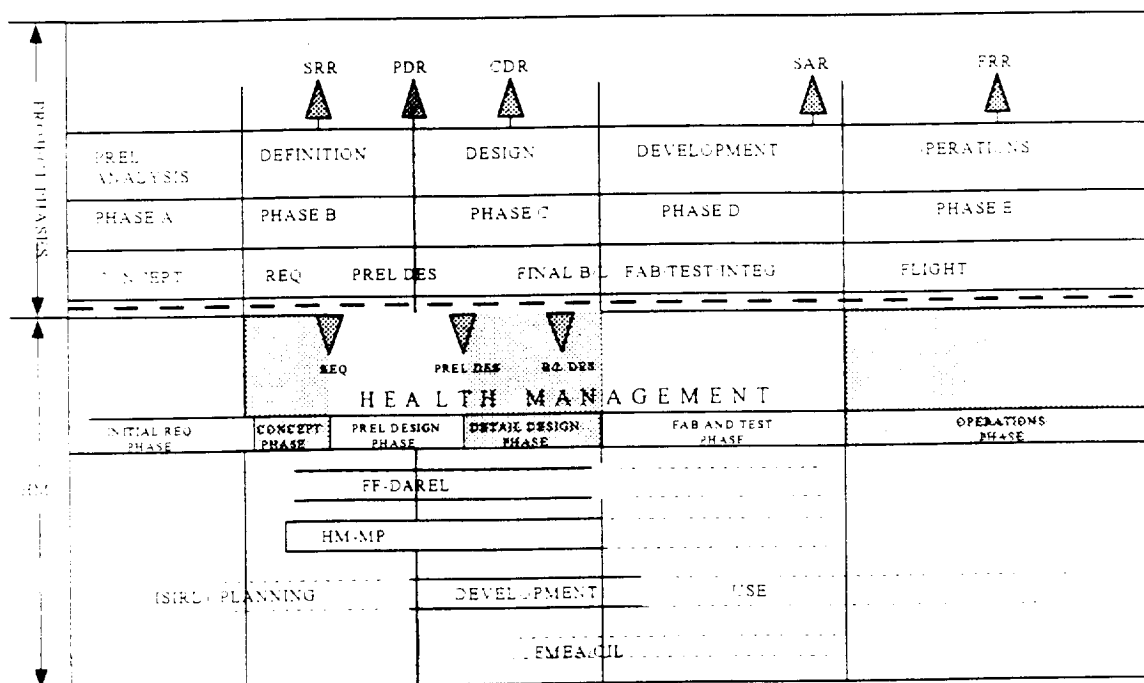


FIGURE III-1. TYPICAL PROGRAM PHASING WITH HEALTH MANAGEMENT

IV.0 DESCRIPTION

IV.1 NARRATIVE (OVERVIEW)

This section of the Handbook presents an Overview of the Processes which can be used in implementing the "Integrated Diagnostic Concept" of Health Management. There are Processes, and efforts, which must be done in each Project Development Phase. Roles of Key Personnel will be identified along with the Processes and will further be developed in Section V-- "Methodology". There are three (3) Key Working Documents which are identified and their purpose is described in this Section, and their development and use is described in the "Methodology" Section. The Health Management Development Process begins with the "Initial Requirements Phase" and proceeds through "Conceptual Design Phase", "Preliminary Design Phase", "Detail Design Phase", "Fabrication and Test Phase", and concludes with the "Operations Phase". Figure IV 1, HEALTH MANAGEMENT FLOW, shows the sequential steps and broad Health Management efforts outlined in this Handbook.

IV.1.1 THE INITIAL REQUIREMENTS PHASE

This Phase encompasses the Project Development Phase A and consists of very fluid and broad efforts and is expressed in Top Level Terms.

- * The System Engineer who has responsibility for Health Management during this Phase assesses the Project Concept, and familiarizes with broad block diagrams and/or mission development timelines

- * The System Engineer searches the available (sometimes being developed) documentation such as "Program Requirements Document", "System Specifications", or "Safety and Mission Assurance Requirements", and "Project Plan" for Health Management relevant information such as Projects Objectives, Technology and Advanced Development Requirements, Targets for

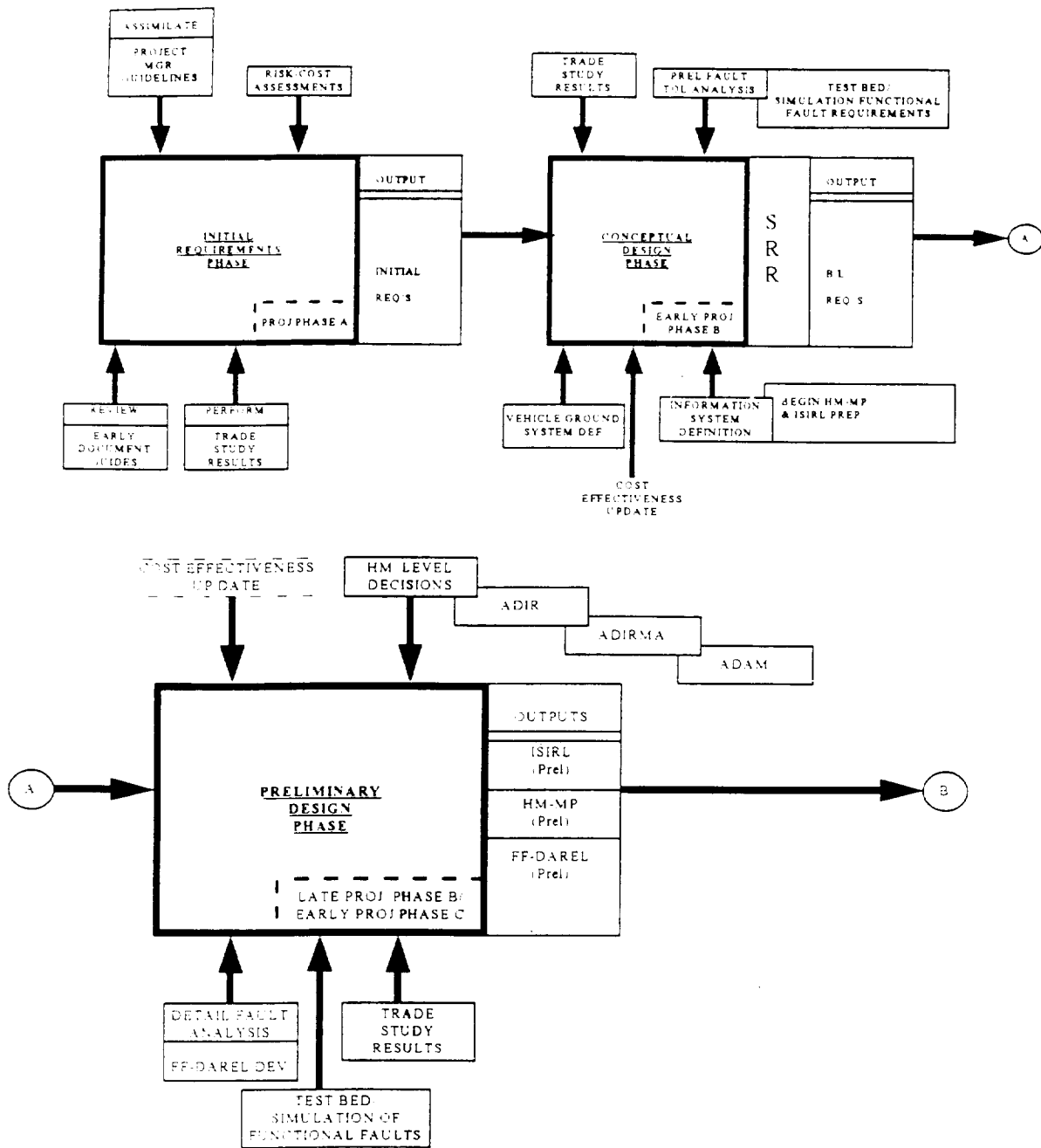


FIGURE IV-1A Health Management Flow

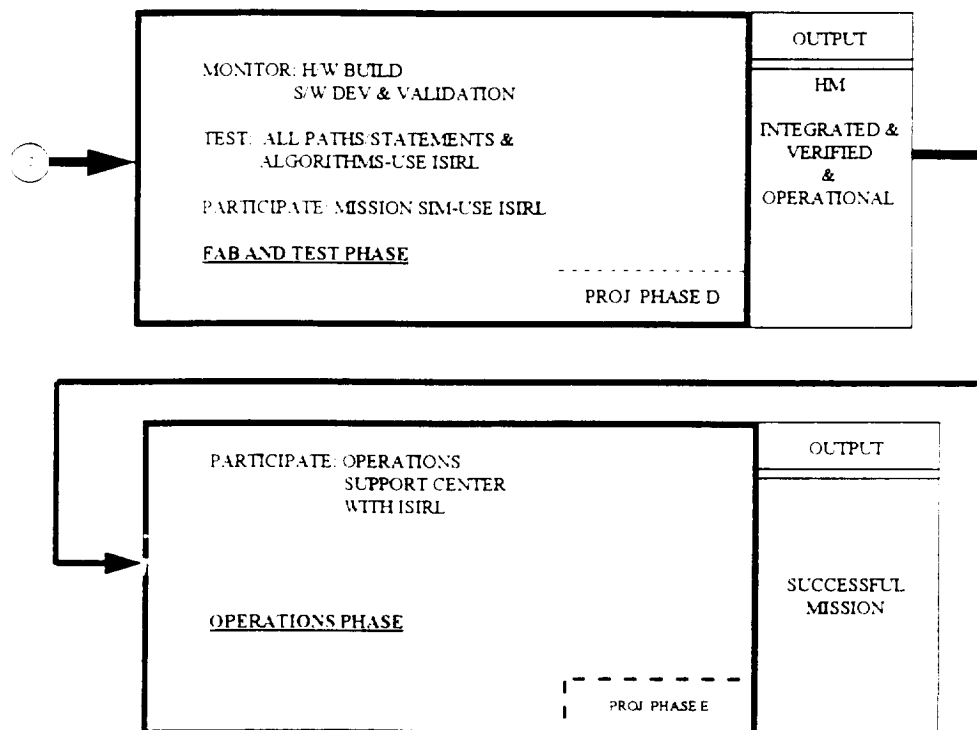
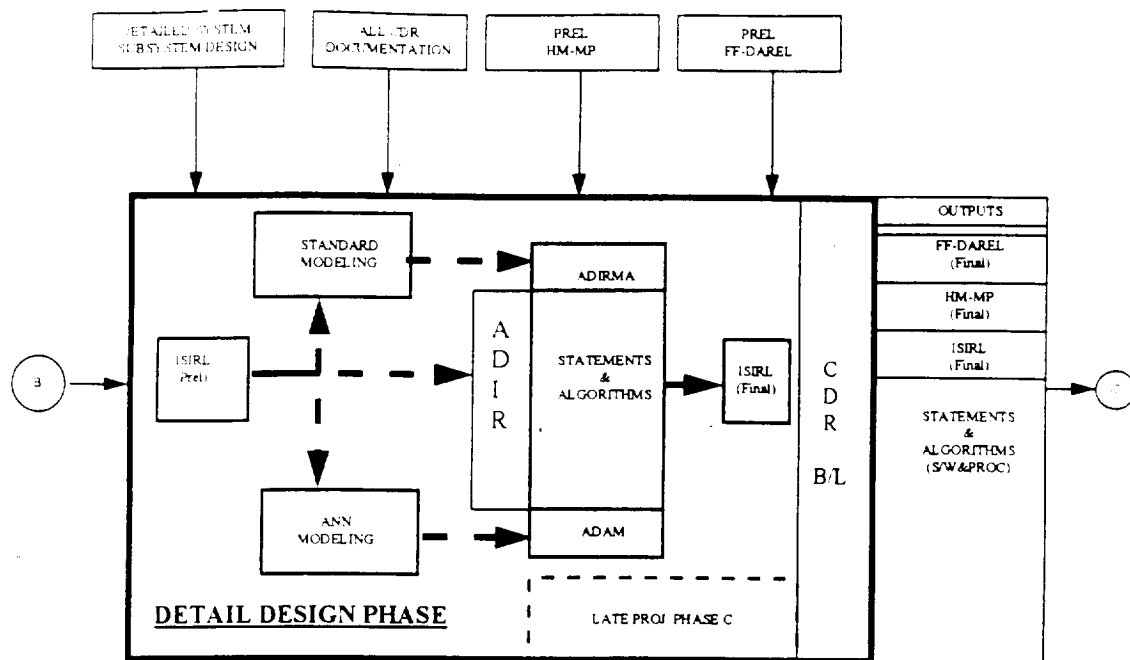


FIGURE IV-1B Health Management Flow

Probability for Mission Success (PMS), Potential Health Management Trades, and Reliability Targets for Sub-Systems. These high level documents often provide insight into the Project plans for maintenance missions, replaceable elements, availability, and any planned reflight, recycling, or refurbishment of the spacecraft. This information enables the System Engineer to evaluate the need for specific HM Requirements to be imposed on the detail design (hardware and software). (See Section IV.1.2.1, Requirements, General & Typical Candidates).

* The System Engineer addresses the need for Trade Studies which would suggest options with relevant Health Management functions for Sub-System Design-These could be initiated by the System Engineer, or more appropriately initiated and controlled by the detail designer, with participation by the System Engineer. Typical Health Management relevant functions which could be addressed during Trade Studies as a prime, or secondary objective are:

- Vehicle (On-Board) Health Management versus Ground Health Management Design Options

- Design alternatives in areas related Health Management, such as:

- +Reliability

- Fault Tolerant, versus

- Fault Avoidance = (Considerations such as cost-complexity-and impact of partial, or complete mission failure)

- Maintainability

- Diagnosibility Considerations and impacts of each
 - Repairability (parameters-spares-storage space/weight
 - Accessibility expertise availability)
 - Supportability

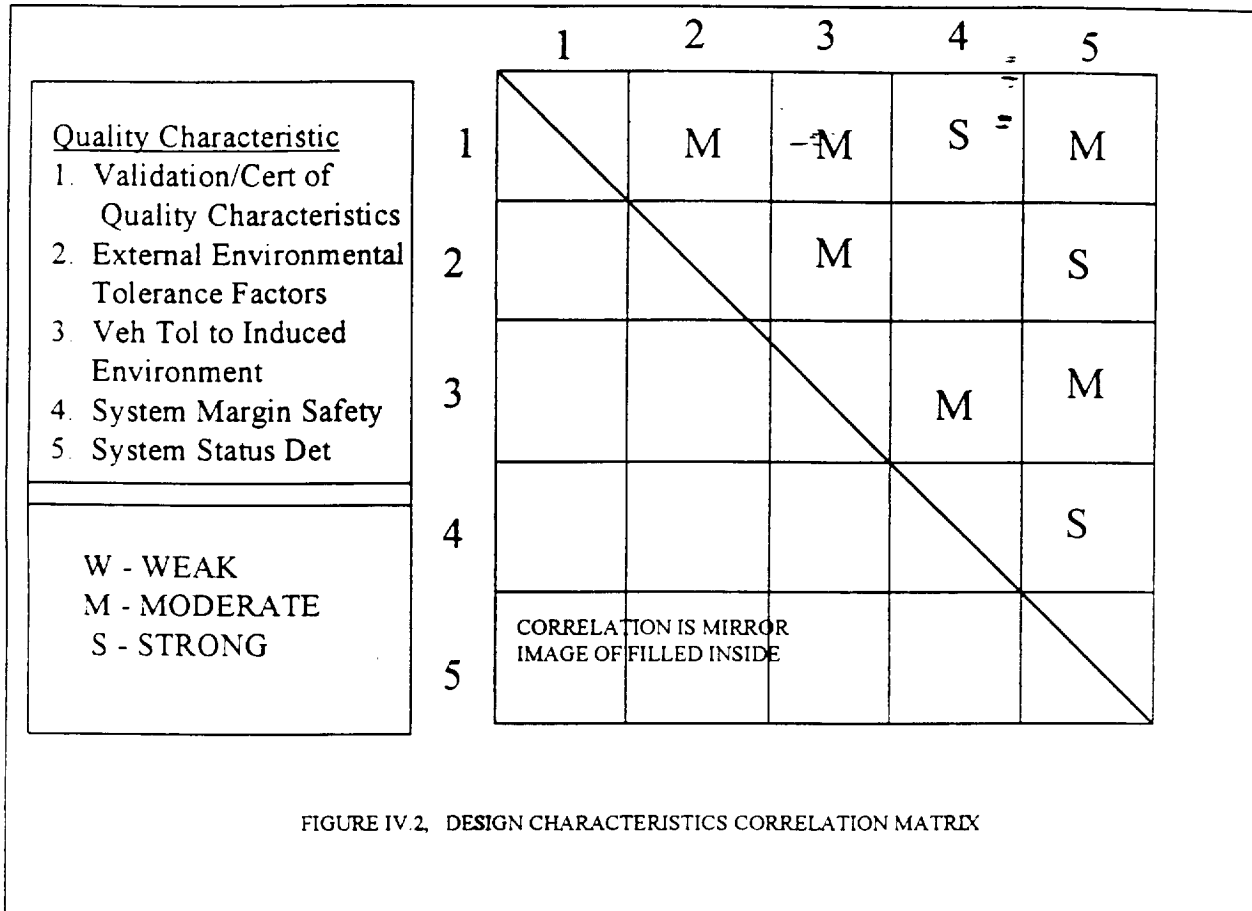
- Information

- That necessary for analysis (typical for similar projects)

- That necessary for trending (typical for similar projects)

- Determination of how much one quality characteristic (such as reliability) can be compromised at the expense of another quality characteristic (such as pointing accuracy) in various controllable aspects of the design. A method to determine the potential desirability of

such a trade study is the Matrix shown in Figure IV.2, Design Characteristics Correlation Matrix. A characteristic which has strong interaction with numerous other characteristics possibly should be studied to determine the degree of acceptable change to optimize the design. (Ref. Doc. 1, RECMS-Martin Marietta, October 30, 1992)



* There are Project Manager Guidelines which must be considered at this early Phase of Health Management activity. The goal of Health Management might be given in terms of "intent"- only recognizing that activity toward accomplishing some degree will be appropriate for that project. Typical constraints which could give insight into the degree of Health Management to be implemented are: Schedule, Resources (Funding-Manpower), Mean Time Between Failure (MTBF), or Mean Time To Repair (MTTR) guidelines. Surge guidelines (capability to respond (a) urgently, or (b) routinely) are other examples of typical Project Managers guidelines.

* Risk/Cost Assessments are typically performed as part of the "Initial Requirements Phase" and are updated as appropriate in the "Conceptual Design Phase."

* The tangible product (or output) of this "Initial Requirements Phase" is the Preliminary Requirements. This consists primarily of a generalized definition of the Health Management concept for the Project and is the first stage in a more detailed Requirement Definition in the next Health Management Phase.

IV.1.1.1 COST EFFECTIVENESS AND RELIABILITY/RISK ANALYSIS

Cost Effectiveness analysis as discussed in this Section of the Handbook is accomplished in the Initial Requirements Phase and is likely updated in both the Conceptual Design Phase and the Preliminary Design Phase.

As stated in the Initial Study (Ref. Doc. 4) and substantiated in many Reference Documents (Ref. Doc. 1 RECMS), Ref. Doc. 21, Boeing Anti-Satellite (ASAT) Mission and System Effectiveness, and Ref. Doc.11, Engineering Design for Producibility and Reliability, John W. Priest, 1988, Marcel Dekker, Inc., there are always costs up front that represent additional program expenditures, however, the savings realized during test/checkout and operations over the Life Cycle more than offset these initial costs. In this case of "Integrated Diagnostic Concept" outlined in this Handbook much of the very much time consuming analysis and decision making that is required during integration, verification testing and operations is accomplished in the early design phases. These choices and decisions are developed into statements and algorithms and translated into software logic and/or procedures for use in the later test/operational phases. Thus, the critical time which might be needed to make these choices and decisions and the possibility of inconsistent decisions in test/operational phases is minimized. A reliable method for arriving at credible cost analysis, or savings, remains a challenge and is always subject to debate relative to accuracy. Tangible cost saving benefits can be more accurately determined for projects that are re-flown and with repetitive operations - where the savings are compounded - however, for projects that need assessments/benefit analysis in early project development phases, or, for one flight mission, a more methodical process must be used and, even then, many assumptions and

later updates are required. An example of the problem relates to the question of redundancy of a critical pressure sensor in a fuel cell - Is the increase in probability of success by providing a redundant sensor enough to justify the extra costs - and are other risks related to having total backup fuel cell capability worth more than incremental redundancy? Schedule constraints and inability to have credible reliability and cost data often take precedence over decisions based on cost alone. So, with these uncertainties in mind, the following simplified method (and guideline tool) for arriving at cost analysis is described.

Cost Effectiveness:

Describes the relative value of a system. It's measure reflects the cost of purchase/manufacture, installation, maintenance of the system over it's useful life and the operational cost while performing it's intended function. It can apply to a subsystem, system, vehicle, payload or an experiment.

So, it can be expressed as:

$$\text{Cost Effectiveness (C E)} = \frac{\text{System Effectiveness (S E)}}{\text{Acquisition Cost} + \text{Utilization Cost}}$$

Where:

System Effectiveness is a measure of the probability that the system can successfully meet an operational demand within a given time when operated under specified conditions.

And

Acquisition costs are those funds expended to attain a specified performance. This includes development cost, production cost, and the cost to ready the system for it's mission after it is produced

And:

Utilization Cost is the predicted, or actual, cost of a mission which used the system with no anomalies.

An Example of the above expression follows.

SYSTEM	COST	FAILURE RATE PER 100	FAILURE RATE IMP.	S.E.	C.E.
PAX Pointing System	100,000	4	--	96	9.60×10^{-4}
PAX Pointing System with	100,960	3	25	97	9.60×10^{-4}
Health	101,920	2	50	98	9.60×10^{-4}
Management	101,000	2	50	98	9.70×10^{-4}

FIGURE IV.3 COST EFFECTIVENESS EXAMPLE

Note: In this example, any Failure Rate Improvement causing a System Effectiveness (S.E.) increase of more than \$960/point is cost ineffective. The last example of \$500/point is shown as a positive cost effective HM effort.

Another method of expressing Cost Effectiveness (C.E.) is:

$$\text{Cost Effectiveness (C.E.)} = \frac{\text{Cost of Improvement (i.e., Health Management)}}{\text{Failure Rate Improvement}}$$

Here, Cost Effectiveness is the cost per unit of Failure Rate Improvement -- (Less Cost Unit of Improvement is more cost effective)

In the above example, the C.E. of Health Management added to the PAX Pointing System is 38.4 in Examples No. 1 & 2 and is 20 in Example No. 3.

The latter expression is less complicated and seems to reflect a more meaningful expression of Health Management effectiveness.

In the above example, it is just a matter of searching/gleaning information on costs to determine Life Cycle Costs, and/or costs of enhancement.

Determining the System Effectiveness (expressed as Failure Rate) is more complicated and is a function of Reliability, Maintainability, Human Factors, Logistics, and other variables (See References for Life Cycle Costs/Risk Management in the Subject Matrix, Appendix II)

IV.1.2 CONCEPTUAL DESIGN PHASE

(These efforts are accomplished in the early part of Project Development Phase B) Systems Engineers and Detail Designers must begin to form a Conceptual Definition of the Health Management design during this Phase. To do this, the early definition of the Vehicle Systems, Ground Systems and, very importantly, the Information System concept (sensors/measurements, signal conditioning, data gathering, data handling/processing/managing and storing and commands) must be studied at the available System, Sub-System, Assembly, and Component Levels. The point of this study is to be aware of what is being planned, and to influence this concept with specific Health Management Design Requirements. It is recognized that, at this stage of Project Development, there may be very little known about the Sub-System, Assembly, and Component Levels, but, to the extent that discussions are being held and broad block diagrams are being developed with functional requirements being assigned to Boxes, the function of Health Management must be included in the appropriate blocks.

* Additional Trade Studies are also appropriate at this Phase. Candidates for Trades (or Investigations) are:

(1) Identification of Fault Containment Regions (Definition: A Region in the System, beyond which certain faults are not permitted to propagate). The purpose of defining Containment Regions is to prevent, by deliberate design (hardware or software), the failure of one functional element from causing failure in other functional areas. If the failure can be contained with 100% certainty -- then the other Functional element would not have to show that particular failure as a Failure Mode. This effort can be significantly cost effective if it is identified and worked in the Conceptual Design Phase.

(2) Passive Fault Tolerance Analysis/Trades are studies of design provisions, and determining those specific designs that can accommodate failure by preventing, delaying, or rerouting the path to a less critical, or already accommodated, path. Examples are "Material Use Selection" and "Physical Containment or Separation" to prevent electromagnetic or heat coupling between devices

** Test Beds and Simulators can be used to further define Functional Faults, Fault Tolerances, and Off-Nominal Functional Faults. It is highly unlikely that Health Management requirements alone could drive the positive need for Test Beds or Simulators. However, if the needs of other disciplines supports their availability and use, then Health Management requirements should lend their support, IDENTIFY REQUIREMENTS FOR, and Plan for their use in the above identified areas in the "Preliminary Design Phase". Fault diagnosability (in terms of whether sufficient sensors/measurements are strategically located to detect identified Functional Faults) can be simulated and analyzed for effectiveness. This Test Bed/Simulation can be the pre-cursor to the "Standard Modeling" (ADIRMA) and "Artificial Neural Network (ANN) Modeling" (ADAM) efforts occurring in the Health Management "Detail Design Phase"

* Fault/Failure Prediction (Trending)--Efforts to identify Functional Faults which can be predicted by Information (parameters, both active and archived) must begin to be identified in this Health Management Conceptual Design Phase. This Information will later be listed in the ISIRL as Statements/Algorithms with all Functional Faults and the methodology which is devised to detect, **PREDICT**, isolate, or recover from these functional Failures.

* Perform Active Fault Tolerant Analysis on each Functional System. Investigation of the Need for Redundant Functions or Redundant Paths is needed to accomplish an acceptable degree of tolerance to an identified failure. The Justification and Criteria for this Need involves many factors and guides should be gleaned from the "System Requirements Document" (SRD), which would be a joint responsibility of the Project Manager, System Reliability, and Health Management. A major input toward justifying this need is the Probability of Mission Success (PMS) goal for the Project along with the Criticality of the identified failure.

****** Preliminary Software Recovery (Sequences) and Data Base Sizing & Timing/Capability--From the results of the Trade Studies, Active Fault Tolerance Analysis, and Trending Analysis, the Detail Designers and Software analysts can begin to scope the necessary detection and recovery software sequences. This allows some initial data base sizing and software effort scoping to take place although the major scoping and sizing efforts will take place in the next Health Management Phase (Preliminary Design Phase)

Note Those Health Management related/supporting tasks, which are noted by "*" can be, and maybe should be, initiated and directed by the System Engineer--but they involve much more than just Health Management factors and absolutely require Detail Designer participation. Those tasks noted by "**" indicate that the prime responsibility should be with the Detail Designer

The PRIME OUTPUT of this Health Management Phase is the generation of a set of Health Management Requirements which are to be Reviewed and Baselined in the "System Requirements Review" (SRR). It should be remembered that this Time Frame is very early in the Project Definition (Preliminary Design) Phase and final details implementing the Requirements are the subject of later documents and review.

IV.1.2.1 REQUIREMENTS (GENERAL AND TYPICAL-CANDIDATES)

GENERAL : Initial Requirements (Preliminary) are identified in the Health Management (HM) Initial Requirements Phase

Final Requirements are identified in the Conceptual Design Phase and are Baselined after Review in the System Requirements Review (SRR)

Requirements must be written to a level of understanding that Sub-System Designers can begin to assess alternatives for Sub-System design.

Requirements begin with Top Level Systems Requirements which may, or may not, have reference to Health Management.

System Engineer would develop next lower tier of Requirements.

Requirements are Related to "Functional Failure" Detection, Prevention, Isolation, and Recovery and must state performance characteristics that can be verified to meet some criteria--OR--they must Require the acquiring of some additional data or product that is specified.

See Section V 5 (Methodology) HM Requirement Generation Process For Developing Specific HM Requirements

TYPICAL/(CANDIDATES):

Functional Requirements:

- Sensors to detect all conditions of Functional Failures must be provided
- Sensors and Data Acquisition providing analysis (on-board or on ground-TBD during the HM Process) must be available and active during all integration, test, and operational phases.
- Environments must be monitored to insure identity of transient and environmentally susceptible functional failures.
- Sufficient sensor and derived data must be available during all integration, test, and operational phases to support anomaly detection, prevention, isolation, and recovery-- Including trending and prediction of anomalies
- The health of the software utilized in HM must be self determined and provided through normal data acquisition--Corrective software routines will be inhibited upon HM software error determination.
- Actual Functional Failures must be distinguished from sensor/data acquisition failures.

- Critical failures will involve the use of multiple limits-with associated multiple levels of criticality
- HM sampling rates (analog) will be at least 2 times the rate at which the failure could occur. Digital signals must be at the same rate at which the failure could occur. Rates must be adjustable (as needed) to allow for increases in suspicious conditions
- Utilize Smart Sensors with BIT capability (Signal Conditioning and other Data Acquisition Hardware should utilize BITE when criticality dictates or when cost effective
- The capability to handle failures (detect-prevent-isolate-recover) must be time or parameter variable if the failure characteristics vary according to mission phase.
- Time to Criticality of all Functional Failures must be addressed and accommodated in Detection/Prevention/Recovery routines
- HM hardware and associated software must be accurate and respond to accommodate 97% of all critical failures
- False accommodation (due to all HM functions) must be less than 1%.

SPECIFIC -- REQUIRED BY THIS HANDBOOK

Develop **HM-MP** (A Health Management Process) per guidelines specified in this Handbook.

Purpose: To document that all "Effects" from Functional Failures can be adequately shown by identified primary measurements or by backup (redundant) supporting measurements.

: To identify and record related measurements

- : To provide a basis for developing the ISIRL (in conjunction with the FF-DAREL)

Develop **FF-DAREL** (A Health Management Process), an "Early FMEA" which supports other Health Management Processes. Its purpose is to identify all Functional Failures, define and record the resulting Effects and insure that measurements are planned which reveal these Failure Effects

Develop **ISIRL** (A Health Management Process) per guidelines specified in this Handbook.

Purpose To document ALL Statements and Algorithms associated with Functional Fault Detection, Prediction, Isolation, and Recovery--AND--the Method of Implementation (Software Logic or by Manual Procedure)

IV.1.3 THE PRELIMINARY DESIGN PHASE

(Late Project Phase B and Early Project Phase C). The conceptual implementation of Health Management into the Project design begins to take form during this Phase which encompasses Project (Late) Preliminary and (Early) Final Design leading to the Critical Design Review and Baselining of the Program Documentation. The effort accomplished during this Phase is critical to implementing an effective Health Management Program.

Results of technical efforts accomplished in the Conceptual Design Phase [Identification of Fault Containment Regions, Fault/Failure Prediction (Trending), Active Fault Tolerance analysis, and Requirements identified and Baselined] are further developed and updated, or validated, along with "Cost Effectiveness" information. This data feeds into, and provides major input for, the "Health Management Level Decision" Process.

The Requirements identified for using Test Beds/Simulators, and centered around Functional Fault Definitions, Fault Tolerances, and Off-Nominal Functional Faults are implemented to further solidify these potential Failure Identifications, Tolerances, and their

resulting effects. The results of this Test Bed/Simulation effort are to be reflected in the "Health Management Level Decision" Process.

It is noted that in Ref. No. 1, RECMS, that hardware faults are due less to "Random Failures" than to "Human Fault in manufacturing, environmental faults, or design faults". If this statement is, in fact, true, then strong emphasis placed on test and verification can detect and eliminate many potential failures before the Operations Phase. The concept described in this Handbook of Health Management is not designed to predict and manage failure due to manufacturing, faulty environmental/other design capabilities. It should be noted that all other identifiable potential Failures, regardless of cause or source, must be addressed in the development of the FF-DAREL, and the method of accommodating the failure is documented in the ISIRL.

Additional **TRADE STUDIES** are appropriate during this Phase.

Examples are:

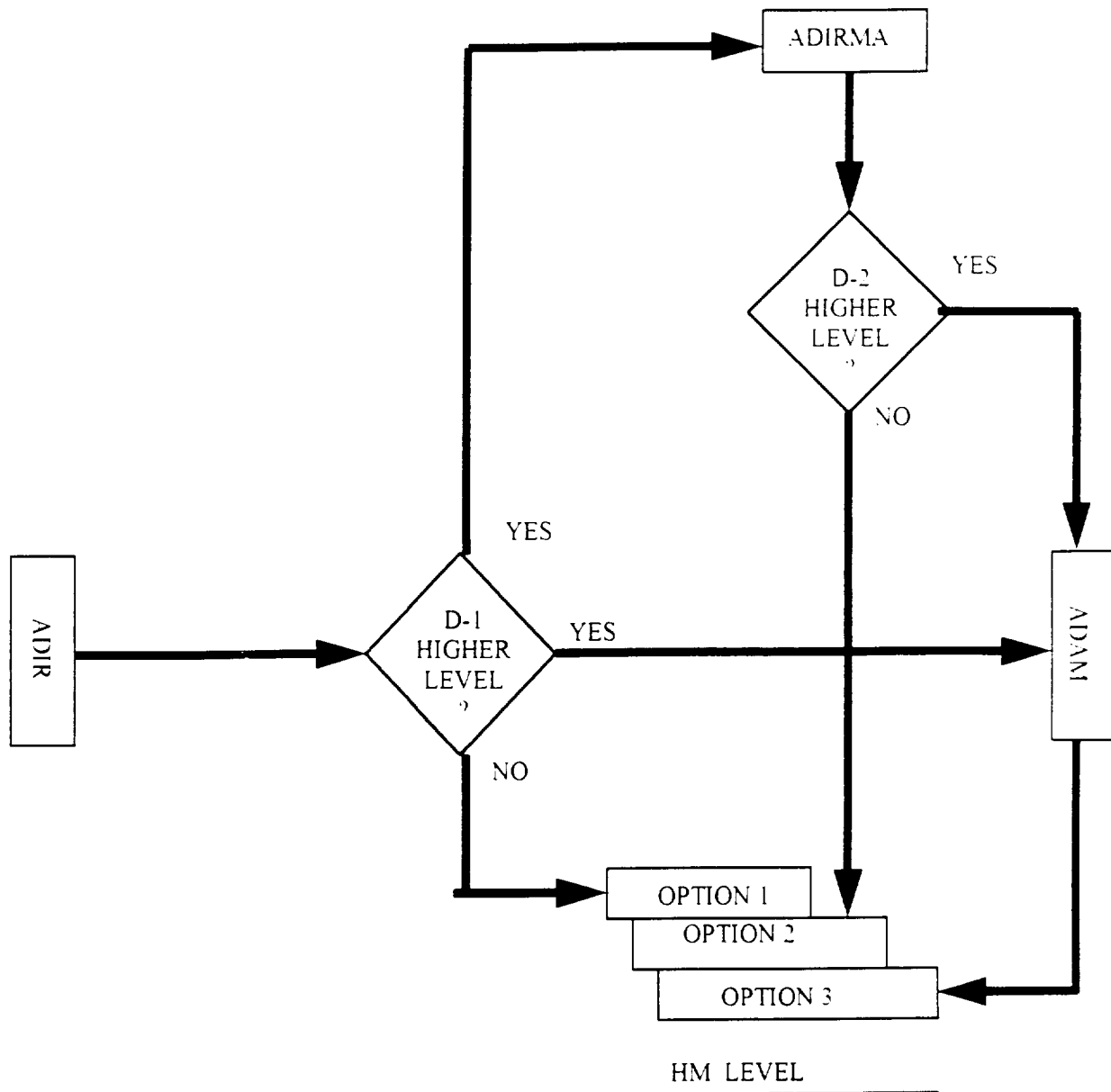
1) All efforts should be made to utilize sensors that are required to provide parameter data in support of operational needs as opposed to dedicated Health Management use. Health Management use of critical control parameters [and the associated sensor(s)] may complicate Health Management Algorithms or Statements to an unmanageable degree. Trades to investigate this possibility and to identify alternatives, such as dedicated, or decentralized sensors and unique software, decoupled from operations, for Health Management use are appropriate.

2) Trade Studies during this Phase to evaluate the need for Redundant Paths and Boxes may be necessary. Considerations for Multiple use Hardware and Software (Mission/Operations and Health Management Use) or Dedicated Hardware and Software for Health Management use only) should be evaluated in certain cases. Critical Functional Failures, earlier identified in Trade Studies may suggest the need for Redundancy of equipment and Paths--Review of this earlier analysis with updated justification, substantiation, and criteria is desirable during this Phase.

Constraints (Cost, Schedule, MTBF, MTTR) that were addressed in the "Initial Requirements Phase" should now be reassessed with the additional maturity of the Project and will be a factor in the "Health Management Level Decision" Process.

Several major Health Management efforts begin in this Phase. Development of the "FF-DAREL" (A Health Management Process) described in Section V 3 of this Handbook is a major working Document and the Preliminary version is one of the primary outputs. All potential/predicted Functional Failures are listed in this Document, along with other necessary information discussed in Section V 3. The "HM-MP" development, began during the "Conceptual Design Phase" is a major development task during this Phase. It includes a total planned Parameter/Measurement listing which will be used to insure that all "Functional Failure Effects" can and will be detected. This Document also supports the sizing and scoping of the Data Base capability. Although it is not finalized until the "Detail Design Phase", its major development, and use, occurs in the "Preliminary Design Phase". The Process detailing its development is also outlined in Section V 2 (Methodology) of this Handbook. The Key Working Document developed for Health Management is the "ISIRL", also a Health Management Process. A preliminary version of this Working Document encompasses the Algorithm/Statement approaches and also documents the Fault Isolation and Response Statements. The Circuitry/Paths and Hardware/Software which is being identified to accommodate all identified Functional Failures, both by Software Logic and by Manual Procedures is included in the Document.

The major decision regarding the Selected Health Management Level of Implementation is determined during this Phase (See Figure IV-4, Health Management Implementation Level Decision). Results from Fault Analysis, Trades, and Test Bed/Simulations, along with Cost Effectiveness data provides sufficient input to determine the most appropriate Level for the specific Project. This Decision Process involves Selecting either (1) Aural Definition of Intersystem Relationships (ADIR), (2) Aural Definition of Intersystem Relationships with Modeling Assistance (ADIRMA), or (3) Aural Definition with ANN (Artificial Neural Network) Modeling (ADAM). This Process is described in Section V.1 along with the Methodology for the other four major Processes.



OPTION 1 (DECISION D-1) = HM LEVEL 1 (ADIR)

OPTION 2 (DECISION D-1) = HM LEVEL 1 (ADIR) AND [LEVEL 2 (ADIRMA) OR LEVEL 3 (ADAM)]

OPTION 3 (DECISION D-2) = HM LEVEL 1 (ADIR) AND LEVEL 2 (ADIRMA) AND LEVEL 3 (ADAM)

Figure IV-4, Health Management Implementation Level Decision

The Primary outputs from this Phase of Health Management Development are Preliminary versions of the HM-MP, FF-DAREL, and the ISIRL. The Major decision, concluded from this Phase, is one of the three Levels of Implementation described above.

IV.1.4 THE DETAIL DESIGN PHASE

(Encompasses Project Development Phase C) This is the most intense Phase in the Health Management Process. Specifically, it involves gathering and assembling the mass information from the Health Management Working Documents (FF-DAREL, HM-MP, and Preliminary ISIRL) into meaningful Statements and Algorithms. All Studies, Trades and the Preliminary Working Documents and the Preliminary Design has been accomplished and the Decision has been made with respect to the Level of Health Management to implement. Now, the Detail Sub-System and System Design is underway in preparation for the Critical Design Review. The Algorithms/Statements and their supporting parameters/measurements, and Redundant Boxes and Paths, and the Preliminary Design with Health Management functions such as Fault Containment and Passive Fault Tolerance provisions has progressed to Final Design. The System Engineer with Health Management responsibility must be keenly aware of the progressing Final Design in order to prepare the ISIRL which implements the selected Health Management Level.

From the progressing Detail Design and from the HM-MP, FF-DAREL, and the Preliminary ISIRL, the Statements/Algorithms are developed which define the fingerprint of the Functional Failures and define the Methods of accommodating (detecting, preventing, isolating, and/or recovering) the failure.

The method of implementing the ADIR Level of Health Management involves detailed discussions with all the Detail Designers which have responsibility for Sub-System design and which have any traceable relationship to any specific Failure. The ADIR Statements and Algorithms must be developed prior to progressing to either the ADIRMA Level or ADAM Level of implementation. **ADIR DEVELOPMENT IS A PRE-REQUISITE TO FURTHER LEVELS OF IMPLEMENTATION**

ADIRMA involves utilizing the ADIR Statements and Algorithms and all other measurements/commands/relationships (not all necessarily involved in Health Management) in Standard Modeling Prediction. The output of this level results in a higher level of confidence that all Information Relationships have been identified and are included in the ISIRL.

ADAM also involves utilizing ADIR (or ADIRMA) Statements/Algorithms and all other measurement/command relationships (not necessarily involved in Health Management) in Artificial Neural Network (ANN) Prediction. This gives additional validity that all Intersystem Information Relationships have been included in the ISIRL and provides a significantly added level of Predicted Fault Detection (Trending) capability.

The result of this Statement/Algorithm development is Documented in the Final ISIRL along with the defined Software Logic implementing the automated Decisions and Choices being developed by the Detail Software Design Personnel. The manual Procedure Decisions and Choices made must be identified as such in the Final ISIRL and will be included in Test/Verification and Operational Procedures.

The System Engineer must insure that testing and verification of all Statements/Algorithms is included in the VRSD. The validation of all Software Logic implementing Algorithms must be included in Software Requirements Documentation.

These implemented Health Management Processes will be subject to review and Baselineing at the CDR and comprise the output of the Detail Design Phase of Health Management.

IV.1.5 FAB AND TEST PHASE

This Health Management Phase encompasses Project Development Phase D, and involves relatively little Health Management Development work. However, the System Engineer must monitor all the Hardware build and assembly to insure that Health Management Design is included as planned and implemented in the documentation. Software Development is also monitored to insure inclusion of all Software Logic related to Health Management Processes for Fault Detection, Prevention, Isolation, and Recovery. The System Engineer participates in Test Operations to the extent of insuring that all Paths/Statements and Algorithms which are included in the ISIRL are verified to be correct and operational. All HM Test Requirements must be accomplished, including off-nominal testing to verify the statements and algorithms in the ISIRL. Mission Simulation Tests should include representative Health Management Decisions and Choices, both by Software Logic (On-Board and Ground) and by manual procedure accomplished by on-board crew and by ground operations.

The output of this Health Management Phase is an Integrated Health Management Operational System, verified and ready to support Mission Operations.

IV.1.6 OPERATIONS PHASE

(Project Development Phase E) This Health Management Phase requires the support to Mission Operations by the System Engineer in/at the Support Center. The ISIRL is the Handbook for providing this support since it includes all potential Functional Failure Detections, Preventions, Isolations, and Recoveries. The System Engineer should be ready to support any Sub-System/System Designer in the role as Operations monitor providing technical recommendations in any off-nominal circumstance. The System Engineer should record all evidence of the role that Health Management Statements/Algorithms played in the operational flow of the Mission. This will provide valuable "Lesson Learned" information and enable future Health Management implementation to be more overall effective.

V.0 METHODOLOGY

V.1 DECISION MAKING PROCESS

Reference Figure IV-4. HEALTH MANAGEMENT IMPLEMENTATION LEVEL DECISION

There are three (3) Levels of HM Implementation These are

- 1) Level 1--Aural Definition of Intersystem Relationships (ADIR)
- 2) Level 2--Aural Definition of Intersystem Relationships with Modeling Assistance (ADIRMA)
- 3) Level 3--Aural Definition With ANN (Artificial Neural Network) Modeling (ADAM)

Those results obtained in Level 1 (ADIR) are absolutely necessary in order to begin, or progress, to Level 2 (ADIRMA) and/or Level 3 (ADAM). However, it is not necessary to perform Standard Modeling (ADIRMA) to progress to the implementation of Level 3 (ADAM)

Level 1 (ADIR) Aural (Gleaning by Personal Communication) Definition is the gathering and Documenting of all applicable (from FF-DAREL) Intersystem Relationships, expressed in terms of Parameters (Identified as a Measurement or a Command). (SEE Process V 4. ISIRL PROCESS) The working Document required for implementing this Level is the BASIC ISIRL. These Parameters are derived by conducting workshops with Detail Designers expressly for the purpose of Identifying Related Measurements and Commands which are Associated with Functional Failures identified in the FF-DAREL, and stating these Relationships mathematically

Level 2 (ADIRMA) is the process of utilizing the Intersystem Relationships identified in ADIR, and all other measurements and commands-which have not been shown to be related to Functional Failures in the FF-DAREL, but may have other internal relationships-in Standard Modeling Prediction exercises. The primary purpose of this effort is to uncover any measurement/command relationship not identified in the Level 1 Aural Definition Process, and to verify/validate the mathematically expressed relationships.

Level 3 (ADAM) Implementation is the Process of, again, utilizing the Intersystem Relationships Identified in ADIR (and ADIRMA, if implemented) in establishing Neural Patterns of Functional Faults. Fault diagnosis using Neural Networks has the same structure as Model-Based methods--but the difference is in the diagnosis technique. The theory and practical application of Artificial Neural Networks (ANN's) is relatively new but is expanding at a very high rate. Fault Diagnosis is one of the most promising applications, and, overcomes some of the shortcomings of Model-Based techniques. The approach requires relatively exact knowledge of the parameters in the Model and calculations can very easily become excessively time-consuming (Ref. No. 9, "Real Time Fault Monitoring of Industrial Processes"--Chapter 5-- (Microprocessor-Based and Intelligent System Engineering) Vol. 12-- By A. D. Pouliezios and G. S. Stavrakakis-- Kluwer Academic Publishers, 1994). These Characteristics must be considered in deciding to implement Level 3 (ADAM), Health Management.

The HM Level Decision Making Process should consider the above Description and Definitions--however--rarely does this type information, alone, provide the answer. The other major factors include: Cost, Schedule, Complexity, and Desired Probability of Mission Success (PMS). The Project Engineer must evaluate ALL considerations and factors and make the Decision.

V.2 HEALTH MANAGEMENT MEASUREMENT PROGRAM (HM-MP) DEVELOPMENT PROCESS

GENERAL. A sample Form of the HM-MP is shown in Figure V-1, HM-MP FORMAT.

The HM-MP has basically the same format and information as the "IP&CL", but it is developed relatively informally, in an earlier time frame, and supports other HM Processes.

Reference Figure 28, MSFC-HDBK-1912A, Vol. 1, Page 85.- The "Preliminary IP&CL" identified in this Process Flow can possibly be the "HM-MP" described in

this HM Process--however, additional supporting information is required for HM purposes (See Figure V-2, HM-MP Process Flow)

Reference MSFC-STD-1924 (IP&CL)

It is not clear as to who is the approval authority for including any given measurement in the design, but it is assumed that the Detail Designer can identify the need, will include it in the design and justify it's need in the SRR, PDR, and CDR, or until Baselineing of the HM-MP at CDR. Neither is it clear what criteria is used for selecting measurements and commands. Health Management requirements and interests can, and should, impact this selection process.

The HM-MP development is a Proactive Process (System Engineer-Lead, but Detail Designer is a major contributor). It is not a CCB controlled Document but one that may be reviewed as part of SRR, PDR, and CDR as supporting information. It is the responsibility of the System Engineer who has responsibility for Health Management to maintain and assure its accuracy.

SPECIFIC In developing the HM-MP, the following questions must be asked and the answers appropriately documented as part of this Working Document (HM-MP).

1) Why is the Measurement/Command required?

- Is it merely to determine proper operation of a system/sub-system?
- Is it to provide scientific information?

There is discrete information and analog value data--are manual, automatic, or no real time decisions required to be made from this measurement? Is it just for Post-Flight data reduction?

2) What is the consequence of the measurement/command failing?

- 3) Is there another measurement (or measurements) which can yield the same, or nearly the same, information?
 - Can the alternate measurement(s) calibration curve (polynomial) be stated as an Algorithm?
- 4) What other measurements are related in any way (Do they vary in any predictable way when the primary parameter varies?) (How can this relation be stated? -In an Algorithm? -Either mathematically, or as $F(x)=F(y) + Z$, where Z is not known, except as $Z = (M-L)$ (L approaches M)
- 5) Who is the Measurement Requestor?
- 6) A Software Parameter List must be generated (measurement or command)--This is a computer generated parameter/measurement/command or a statement/algorithm expressed in message structure form.
- 7) The standard IP&CL measurement/command list includes the following information which is also required in the HM "HM-MP"
 - Measurement/Command Name and Number
 - Sample Rate Required (Function of Frequency Response)
 - Accuracy - Stated in Terms (+ or -) % of Full Scale
 - Range (in Engineering Units)
 - Communication Path and Data Address
 - Command Verifier (Measurement)

HM-MP

Measure No. or Command No	MEASUREMENT NAME OR COMMAND NAME	SIGNAL TYPE	SAMPLE RATE	NO OF BITS	RANGE (EU)	ACCURACY OR COMMAND BIT CONFIGURATION
1 - 11	12 - 51	52	53 - 54	55 - 56	57 - 73	74 - 83
ITEM NUMBER 1 - 2 SYSTEM OR PAYLOAD OR ORG-CLASS OR ASS-CLASS DESTINATION, SIZE, NO. OF TYPE OF MEASUREMENT OR COMMAND	NAME	SIGNAL TYPE	SAMPLE RATE	BITS WORD	RANGE IN ENG UNITS	ACCURACY (%LS) OR COMMAND BIT CONFIGURATION
PAN POWER DIST # 1 0008 (TEMP MEASUREMENT #)	SURFACE TEMPERATURE	A ANALOG B BIFLEX C DIGITAL	10 S S	OR	25 C - 15 C	2 %LS 0.7 C OR 01010101
EXAMPLES						

HM-MP

DAS OR COMMAND VERIFIER ADDRESS	NEED (USE)	CRITICALITY	RELATED MEASUREMENTS	DIRECTLY RELATED	SW PARAMETER	MEASUREMENT REQUESTOR
84 - 103	104 - 173	174 - 193	194 - 213	214	215	216 - 245
ITEM DRY DAS or COMMAND VERIFIER ADDRESS	JUSTIFICATION	CONSEQUENCE	YIELD DIRECT OR INDIRECT DATA	YES OR NO	YES OR NO	NAME ORG
AN-AN-AN-AN	-SCIENTIFIC INFO -STATUS -FLAGS -POST FLIGHT -REDUCTION -CONFIGURATION	-CRITICAL RESULTS -DAMAGE OR -DISRUPTION OF -OPERATIONS -NON CRITICAL -PLEASE CRITICAL	-EXPRESS DIRECTLY -PREDICTABLE ONLY -TO DIRECTIONS OF -SHIFT -CAN BE CALIBRATED	YES	NO	BOBFB10
EXAMPLES						

FIGURE V-1 HEALTH MANAGEMENT MEASUREMENT PROGRAM FORMAT

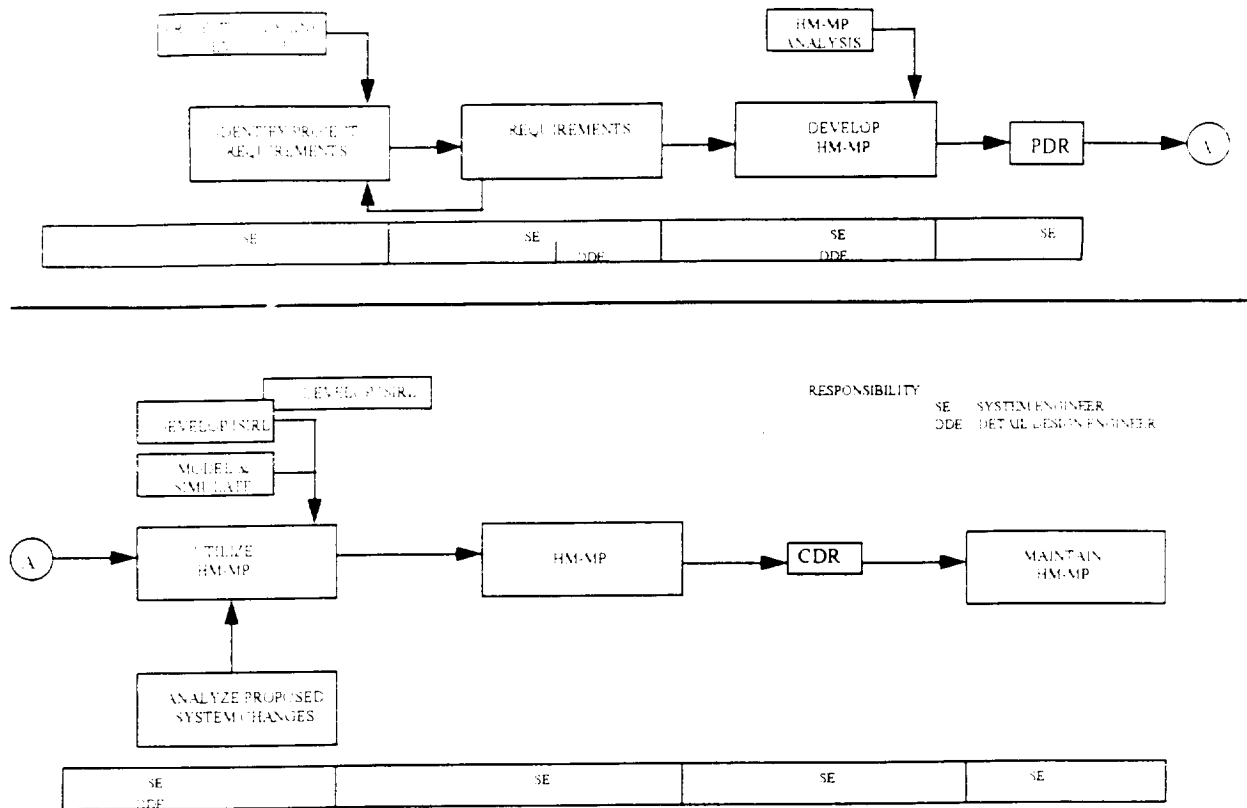


FIGURE V-2 HM-MP PROCESS FLOW

V.3 FF-DAREL DEVELOPMENT PROCESS

GENERAL : The FF-DAREL is the FMEA for HM

- : The purpose of the FF-DAREL is to list all possible hardware Functional Failures. It is developed by Systems Engineering and Detailed Designers. It identifies Hardware and Software interrelationships which allow tracing failure propagation through all hardware levels. It is a Process which follows the Standard FMEA activities outlined in NHB 5300.4 (1D-2) and summarized in the "Specific" paragraph below.
- : The FF-DAREL must be developed during the HM Preliminary and Detail Design Phases, as opposed to the FMEA/CIL activity which is developed to the "as-built" configuration and takes place just prior to, and just subsequent to the CDR (Ref NHB 5300.4).

- : FMEA's goal is to identify failure modes/effects and to perform corrective action by implementing design, or by procedure change. FF-DAREL identifies Functional Failure Modes and Effects and has the goal of recognizing, isolating, preventing or recovering from the failures by planned action during the mission.
- : FF-DAREL addresses Functional Failures without regard to criticality. Those Functional Failures which are later determined to be Criticality 1 or 1R by FMEA will be addressed only to the scope of HM in this Process-but FMEA Processes/Corrective Action may take precedence and override, or alter, the HM approach.
- : HM identified Functional Faults cannot (alone) cause Design Changes. But, since FF-DAREL evolves through Preliminary and Detail Design, changes can occur by the Detail Designer without CCB action prior to CDR.
- : If there are definitely Criticality 1 and 1R Failures identified, the System Engineer, responsible for HM, will insure that the S&MA and Project Manager are aware of the Failure possibility and that they are addressing it through the normal FMEA/CIL Process.
- : The System Engineer and Detail Designers, during the development of the FF-DAREL, will not assume that the crew will perform (or respond) to any Failure Effect observed, nor will they take any Corrective Action unless the Time Criticality is such that it is absolutely certain that Corrective Action can successfully take place.
- : Structural Failures, and Passive Components, such as TPS, are not to be considered in the FF-DAREL development. However, Pressure Vessels are to be included, but only to the extent of instrumentation and signal conditioning.

Seals, barriers, hoses, tanks, lines, ducts, are not to be considered in the FF-DAREL

- : A Table, showing Redundant, or Back-up Hardware, will be developed
Details of how to switch in, or place it in operation (such as a Software command) must be included in the FF-DAREL and the command, if utilized, will be included in the HM-MP
- : "Success Paths" (Redundant Paths) will be listed and "Like" or "Unlike" Hardware located in the Paths being identified.
- : Definition--"Like" Redundancy = Identical Hardware Items and "Unlike" Redundancy = Non Identical Hardware performing the same function
- : Manually emplaced LRU's need only to be listed. No planned utilization is addressed in this HM Concept. Assume that they will operate properly if placed in the System.
- : See Figure V-3, TYPICAL FUNCTIONAL FAILURES (Key Words).
- : Typical causes are listed in Figure V-4, TYPICAL FUNCTIONAL FAILURE CAUSES (Key Words)
- : Propagation of Failures from one Sub-system to another must be analyzed with both Designers (or both sub-system boxes) if the same Designer is responsible for both boxes.
- : Time to criticality will be addressed on each Functional Failure.

TYPICAL FUNCTIONAL FAILURES

Erratic Operation	Premature Operation
Fails to Remain Open/Closed	Delayed Operation
Fails Mid-Travel	Erroneous Output
Fails to Open/Close	Partial Output
Fails Out of Tolerance	Open (Electrical)
Inadvertent Operation	Leakage (Electrical)
Intermittent Operation	Loss of Output
Internal/External Leakage	Fails to Switch
Physical Binding/Jamming	Shorted
Restricted Flow	Fails to Start/Stop
Structural Failure (Rupture)	

FIGURE V-3. TYPICAL FUNCTIONAL FAILURES

TYPICAL FUNCTIONAL FAILURE CAUSES

Acoustics	Ionizing Radiation	Loss of Input
Contamination	Temperature	Vibration
Erroneous Input	Partial Input	Electromagnetic Fields
Mechanical Shock	Thermal Shock	Piece-Part
		Structural Failure
Overload	Acceleration	Chemical Reaction
Vacuum	Pressure (High/Low)	

FIGURE V-4. TYPICAL FUNCTIONAL FAILURE CAUSES

SPECIFIC

- 1) The Process starts by defining the sub-system/system and it's performance requirements.
- 2) Block Diagrams are developed which represent simplified models of the sub-system/system
- 3) Utilize the ANALYSIS WORKSHEET (See Figure V-5, FF-DAREL WORKSHEET) Complete this Worksheet for every identified Functional Failure
- 4) Every element (Usually a Box) in the System being analyzed must be addressed Identify the Box by nomenclature and by Ref. Des. Number.
- 5) "Like" and "Unlike" Redundancy hardware and paths must all be identified and listed in the FF-DAREL.
- 6) The "Effects" or result of the Functional Failure are documented on the Worksheet and all measurements which reveal those effects are identified and listed.
- 7) The following Information is required for each Functional Failure identified
 - Mode (Time) = Premature Operation
 - = Failure to operate at required time
 - = Failure to cease operation at required time
 - = Failure during operation
 - Cause = Identify the cause
 - Effect = List all effects and measurements which indicate the effects
 - Related Measurements = List any "related" measurements which will definitely give an indication, but "may" or "may not" be prime information sources for revealing the Failure State whether these measurements are a reliable source or a questionable informational back-up

source of data which could be used to either "question" the validity of the Prime measurement or to "validate" the Failure Effect

-Time To Effect = Indicate the Shortest time before effects will be indicated
(i.e. Immediately, later in mission, etc.)

-Corrective Action = Identify Actions (automatic and manual) which be taken to circumvent failure

-Time for Corrective Action = Indicate the maximum time to perform Corrective Action before opportunity is lost.

The FF-DAREL consists of the Worksheets as described above and Tables which include supporting information. They are critical to development of the ISIRL, the KEY HM Document

FUNCTIONAL FAILURE - DEFINITION AND RESULTING EFFECTS LISTING
(FF-DAREL)
WORKSHEET
SHEET 1

SYSTEM _____ MISSION PHASE _____ PRE-LAUNCH FF NO: _____ PAGE _____
 SUBSYSTEM/ASSY _____ ASCENT
 COMPONENT EQUIP _____ DEPLOYMENT DATE _____
 DRAWING SCHEMATIC _____ OPERATIONS
 REF DES _____ CONTINGENCY/RETURN

FF NO	FUNCTION DESCRIPTION	FAILURE CAUSE DEFINITION	RESULTING EFFECTS	TIME TO EFFECT	TIME FOR CORR ACTION

FIGURE V-5 FF-DAREL WORKSHEET (PAGE 1 OF 2)

(FF-DAREL)
WORKSHEET
SHEET 2

FF NO: _____ PAGE _____
DATE: _____

S/W ACTION REQUIRED	CORRECTIVE ACTION PLANNED	REDUNDANT/BU HARDWARE	INDICATION MEASUREMENTS

SUMMARY-(SIGNIFICANT FAILURE INFO): _____

CONCLUSION: _____

FIGURE V-5 FF-DAREL WORKSHEET (PAGE 2 OF 2)

V.4 INTER-SYSTEM INFORMATION RELATIONSHIP LISTING (ISIRL) DEVELOPMENT PROCESS

The purpose of this Process is to document all Functional Failure Indications (Detection), Prevention, Prediction, Isolation Measures, and Recovery Actions. The ISIRL is the KEY Working Document (a Manual consisting of all ISIRL Sheets) for HM support during the Fabrication/Test Phase and the Operations/Mission Phase.

It is developed in conjunction with the two other HM Working Documents [The Health Management-Measurement Program (HM-MP), and the Functional Failure-Definition and Resulting Effects Listing (FF-DAREL)]. Development of this Manual begins in the "Conceptual Design Phase" (Reference Figure III-1) with the Preliminary Version being an output of the "Preliminary Design Phase". The Final ISIRL is the Key output of the "Detail Design Phase".

The ISIRL Document (See Figure V-6, Typical ISIRL Format) lists all Statements and Algorithms associated with each Functional Failure (Fault) which was identified in the FF-DAREL. The Statements and Algorithms and other identifying data define the "Fingerprint" of the Functional Failure and define the planned method of accommodating the failure. The ISIRL Document implements and documents all data gathered regarding each Functional Failure (Detection, Prevention, Prediction, Isolation and Recovery) and the indications, inter-relationships, and actions to be taken derived from the selected Level of HM Implementation (See Section V.1) Implementation, as outlined in this ISIRL, maybe by (1) Software Logic, or, by (2) Manual Procedure.

The ISIRL Manual consists of sheets for each Functional Failure and defines, at least, the following information:

- Functional Failure No. (from FF-DAREL)
- Functional Failure Definition (Narrative)
- Functional Failure Detection (Indications)
(Measurements and Values)
- Preventive Measures Planned

-- Planned Recovery Actions (Narrative)

(S/W Logic Routine Description--and/or Manual Procedure Steps)

Primary and Redundant circuitry, paths and functional elements (boxes) are identified and the measurement(s) and values will be identified to insure that (1) the Sensor/Acquisition system is not at fault, and (2) that the planned action is taken within the "Time for Corrective Action" and that the present configuration, and any Commands given are indicated by planned, identified measurements with predicted values.

Again, this Manual consists of all the information required to assist Test and Operations Control personnel in the real-time on-line activities. Software Routines (operating by automatic sequencing, behind the scene, and as part of the normal time-line sequence) are also to be included if they are required to accommodate (Detect, Prevent, Predict, Isolate and Recover) the Functional Failure

FIGURE V-6
ISIRL
WORKSHEET

Basic Sheet ____
Continuation Sheet ____
Sheet No ____

FUNCTIONAL FAILURE NO (FROM FF-DAREL) _____

FUNCTIONAL FAILURE DEFINITION (NARRATIVE) _____

FUNCTIONAL FAILURE DETECTION (INDICATIONS)

MEASUREMENTS (PRIME)

VALUES (LIMITS/DELTA)

MEASUREMENTS (ALTERNATE)

VALUES (LIMITS/DELTA)--RISK

PREVENTIVE MEASURES PLANNED (STEPS)

ISOLATION MEASURES TO BE TAKEN (STEPS)

PLANNED RECOVERY ACTIONS (NARRATIVE)

S/W ROUTINES (NAME)

PURPOSE (SEE NOTE 1)

MANUAL PROCEDURES (SEE NOTE 1)

STEP 1 _____
2 _____
3 _____

NOTE 1 THESE ACTIONS ARE PREFERRED TO BE STATED BY ALGORITHMS OR STATEMENTS WHICH ARE PRE-DEVELOPED AND ONLY REQUIRE INITIATION--BUT MAY BE MANUAL STEPS.

V.5 HM REQUIREMENTS GENERATION

INTRODUCTION

The task of insuring the design of HM into a system, is described here in is a four step process which parallels and sometimes is interleaved with the normal system engineering process. This process assumes that the functional analysis has been completed and that a concept has been selected. The first step of the process is to decompose and allocate system requirements to the appropriate subsystem. The second step is to synthesize the system. The third step is to evaluate and make a decision based on the alternatives. The final and fourth step is to describe the system elements in the form of specifications and plans. Figure V-7 is a flow chart which depict the engineering Process involving Health Management.

DECOMPOSE CONCEPT (FUNCTIONAL ALLOCATION)

Decompose the system into configuration items until a level is reached at which a specific hardware item or software routine can fulfill the intended HM performance requirements. Some straight forward decomposition of the system can be made, but the procedure may involve the use of supporting analyses and simulations to allocate system level requirements. The subject of supporting analyses will be discussed later. But at this point, HM requirements, if unknown, should be assumed using one's engineering experience. A time line analysis of the system will provide insight into the selection or derivation of some HM requirements. Hence, a time line analysis should be performed on the decomposed concept.

The time line analyses is used to determine timing requirements for time critical functions with associated tolerances, determine trade-off process between man and machine, identify what processes should be autonomous, develop trade studies in areas other than time considerations such as whether the spacecraft navigation should be located on the ground or onboard, and estimate HM requirements. The time line analysis is used to derive lower level HM subsystem requirements for each configuration component. HM requirements should be documented so that each HM requirement is identified, its source, and show the allocation to the next lower level.

SYNTHESIZE THE SYSTEM

The purpose at this point of the process is to strike a balance among functional performance requirements, system constraints, and mission success criteria (expressed mathematically as the Probability of Mission Success [P(MS)]) in determining the appropriate HM design concepts. Synthesis, or conceptual design, is the activity which assures that system influences, along with HM requirements, are given the proper consideration in arriving at a design concept. Engineering creativity and technology are brought to bear in the creation of a system or design concept which best meets the stated system HM requirements. Synthesis considers the results of various technical and design studies. HM, being an integral part of system engineering, has input into the design process.

The means by which the system is synthesized can be either be physical or mathematical. The synthesizing process requires that engineering organize, evaluate, and examine the validity of the thought processes. The use of the process permits an optimization of HM hardware and software parameters, allows performance predictions of subsystems to be made, and permits operational HM sequences to be derived.

SCHEMATIC BLOCK DIAGRAMS

A schematic block diagram (SBD) is one of the primary tools for the system synthesis by serving as the basis for models of the system. They are developed, with HM in mind, at successively lower levels as analysis proceeds to define lower level functions within higher level requirements. The SBD shows selected functions and data interfaces within the system. The SBD is used to develop Interface Control Documents (ICD), provide all overall understanding of system operations and to provide a basis for the integration of the HM function. A key goal of HM is to influence the design of modular units which implement a single independent function, performs a single logical task, has a single entry and exit point, and is separately testable.

PHYSICAL MODELING

Physical models can be either full size, scale, hardware, or analog representations of the system. Where human interaction is involved in HM, such as manned vehicles or control consoles, the models are frequently built full size. HM engineering use them to verify controls, and response times as well as to establish maintainability characteristics and ensure maximum efficiency of operation. Full scale models are also used by designers to provide a three dimensional representation of complex structures to facilitate design of features such as cable harness routing, box placement, and access opening locations. As an example HM would have input to box placement. If the box is placed in an hostile environment, then HM would derive more stringent HM requirements for the box. On the other hand, HM could influence the placement of the box in a favorable environment. Breadboards or brassboards are another use of physical modeling where the model is used to provide proof of HM functional operation or to establish critical performance characteristics.

MATHEMATICAL MODELING

A mathematical model is an abstract representation (without regard to physical implementation) of a system. A model will provides a means of developing quantitative HM performance requirements from which candidate designs can be developed. There are basically two types of mathematical models, static and dynamic.

Static HM model are those that depict conditions of state, such as the loading of a mechanical structure. If the equilibrium condition is changed by altering the loading conditions, new values for the load paths may be obtained analytically, but the model does not indicate the manner in which the load paths achieved their new state. Should it be desired to optimize the load paths according to the capability of structural members, a numerical solution would be required.

Dynamic HM models are used to depict conditions that vary with time. But the systems engineer with HM in mind need to depict the random occurrence of faults of a systems that vary discretely or continuously with respect to time and space. Simple dynamic models can be solved analytically but as the system increases in complexity numerical methods are necessary. Because

of the availability of inexpensive computer hardware, HM parameter simulation is less costly than building and testing an actual system

EVALUATION AND DECISION

It should be stated that the intent is not to constrain the system engineer but to provide a basis for his thought process. Engineering innovation is encouraged. Deviation, as required, from the process is the engineer's prerogative.

DESCRIPTION OF SYSTEM ELEMENT

At this point in the process, engineering knows how HM is to be implemented at the system level. Such factors as system interfaces, interoperability, communications function, personnel functions, etc. are known. Special purpose HM equipment should be defined and described how they fit into the "as built" configuration. For those cases where HM functions are an innate part of the system, these functions should be described and shown how they fit into the overall system. HM data flow must be defined and shown how HM data permeates through the system. The following is a list of candidate items which should be included in the system element description

- 1) Health Management Data Flow indicating what decisions are needed at distinct times and locations in the overall vehicle infrastructure, associated information needs, and how the information is collected, stored, and distributed. This plan is prelude to the Instrumentation Program & Command List (IP&CL).

- 2) Overall Verification and Validation should be formulated to verify that the design provisions for active fault accommodation are effective in the operational environment. Planning for a software, and later, a full hardware/software simulation of the Health Management System is necessary to support verification. This plan is the prelude to the Verification Plan.

- 3) Decision on the degree for human interaction in the HM decision making process

4) Software drivers, language preferences, data storage, throughput, protocol, and similar information impacting the overall system software plan needs to be input to the system design level

5) Passive fault tolerance requirements, where special hardware design features are to be used to achieve passive fault tolerance, are identified. These HM requirements need to be integrated into the total system level design process.

6) Requirements that must be incorporated into the simulation testbed to support the HM design process.

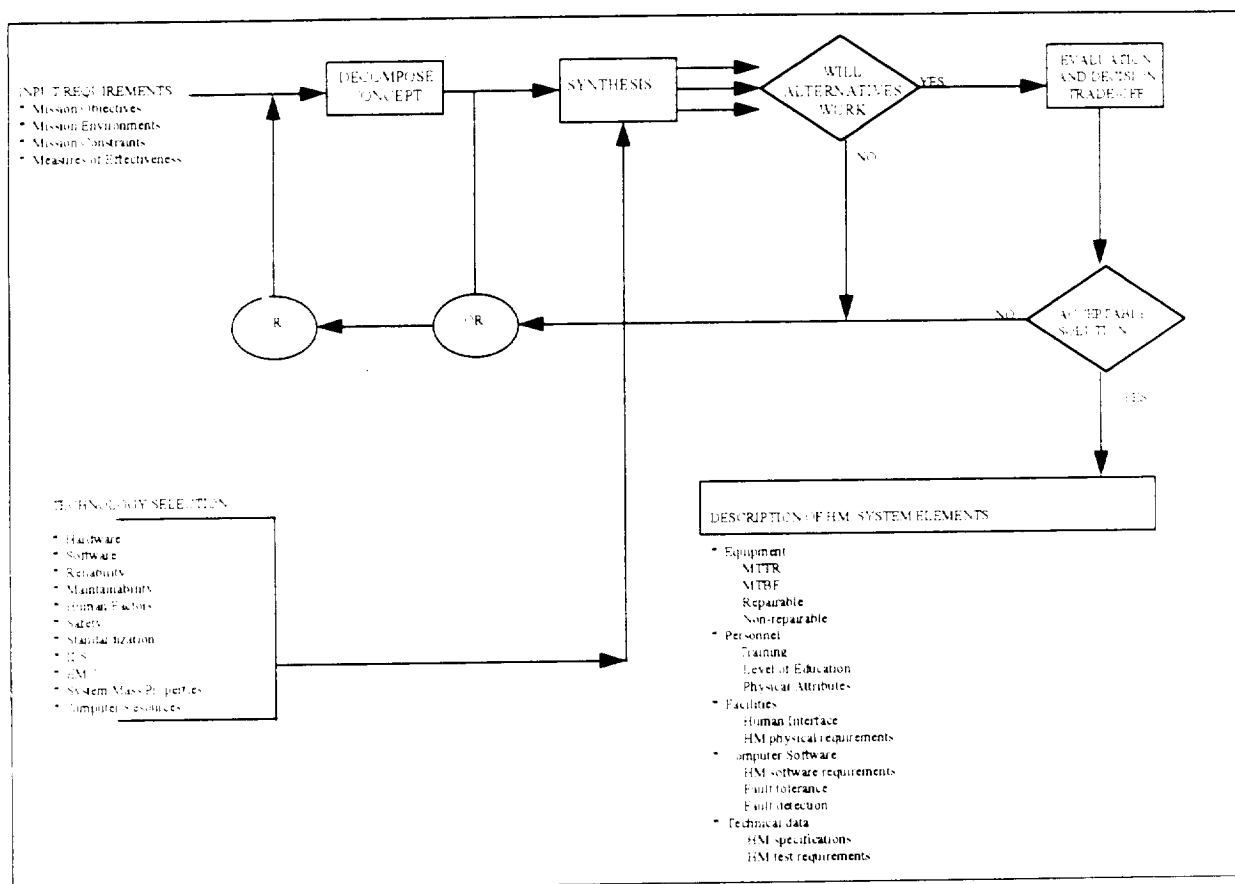


FIGURE V-7. HEALTH MANAGEMENT SYSTEM ENGINEERING PROCESS

APPENDIX I

TABLE AI-1

MATRIX
HEALTH MANAGEMENT PROCESSES
TO
EXISTING SECTIONS OF SYSTEM ENGINEERING
HANDBOOK
(MSFC-HDBK-1912A)

HM SUBJECT (SECTION)		SE SUBJECT (SECTION)	
INTRODUCTION	(I.0)	INTRODUCTION	(1.0)
PURPOSE	(II.0)	PURPOSE	(1.1)
SCOPE	(III.0)	SCOPE	(1.2)
DESCRIPTION			
INITIAL REQUIREMENTS PHASE	(IV.1.1)	PRE-PHASE A	(2.2.1)
CONCEPTUAL DESIGN PHASE	(IV.1.2)	PHASE A	(2.2.2)
PRELIMINARY DESIGN PHASE	(IV.1.3)	PHASE A B	(2.2.2.2.3)
DETAIL DESIGN PHASE	(IV.1.4)	PHASE B C	(2.2.3.2.2.4)
FAB AND TEST PHASE	(IV.1.5)	PHASE D	(2.2.5)
OPERATIONS PHASE	(IV.1.6)	PHASE E	(2.2.6)
DECISION MAKING PROCESS	(V.1)	PRELIMINARY DESIGN	(3.3)
HM-MP DEVELOPMENT PROCESS	(V.2)	SYSTEM REQUIREMENTS DEFINITION AND ALLOCATION	(3.2)
FF-DAREL DEVELOPMENT PROCESS	(V.3)	SYSTEM REQUIREMENTS DEFINITION AND ALLOCATION	(3.2)
ISIRI DEVELOPMENT PROCESS	(V.4)	PRELIMINARY DESIGN	(3.3)
HM REQUIREMENTS GENERATION PROCESS	(V.5)	DETAIL DESIGN	(3.4)
		SYSTEM REQUIREMENTS DEFINITION AND ALLOCATION	(3.2)

APPENDIX I (Cont)

HM SUBJECT (SECTION)		SE SUBJECT (SECTION)	
HM-MP FORMAT (2 SHEETS)	(FIG. V-1)	VOL 2 PROCESSES & CHECKLISTS	(5.2)
FF-DAREL WORKSHEET	(FIG. V-5)	VOL 2 PROCESSES & CHECKLIST	(5.2)
ISIRI WORKSHEET	(FIG. V-6)	VOL 2 PROCESSES & CHECKLISTS	(5.2)
HM SE PROCESS	(FIG. V-7)	VOL 2	(2.2)

APPENDIX II
MATRIX
HM SUBJECT
TO
REFERENCE DOCUMENT

SUBJECT	REF. DOC. NUMBER
ALGORITHM	3, 14, 15, 16, 17, 24, 35
SYSTEMS ENGINEERING	10, 12
TRADE STUDIES	1, 6, 7, 28
SYSTEM SYNTHESIS	6
LIFE CYCLE COSTS/RISK MANAGEMENT	1, 6, 7, 10, 11, 21
TIME TO CRITICALITY	1, 28, 30
HM REQUIREMENTS	1, 7, 30
FAULT PROPAGATION/CONTAINMENT	1, 2, 28
STANDARD MODELING	1 (APPENDIX D), 10, 18
ARTIFICIAL NEURAL NETWORKS	9 (CHAPTER 4, 5, & 6), 13 (SEE APPENDIX III 2) 18, 20 (SEE APPENDIX II 1), 23
RELIABILITY/AVAILABILITY (MTBF-MTTR)	2, 11
DIAGNOSTIC INFORMATION PROCESSING	4, 26, 29
REDUNDANCY	4

APPENDIX III.1

STATE-OF-THE-ART HEALTH MONITORING TECHNIQUES ON BOARD NAVAL VESSELS

Approach

A review of the document revealed that their approach was health or condition monitoring and reporting of a fault when it occurred. The basic philosophy was to approach the technique step-wise. Several types of analytical techniques were used to monitor the naval diesel engine. The approach was to parallel the techniques used by the engine room personnel such as sight, sound, smell, and touch (vibration, temperature). Some of the reasons for this approach were

- 1 The experienced operator is able to 'measure' simultaneously a number of relevant signals (smell, noise, vibration, temperature, smoke) in a three dimensional continuous field
- 2 In many cases the sensitivity of the 'measurement' may be high.
- 3 The experienced operator evaluates, trends and combines the measured signals and, as a result, gives, in many cases, a correct diagnosis."

Success

The study showed a great deal of success. A great deal of information can be obtained from health or condition monitoring. The Royal Netherlands Navy used the concept to augment their maintenance of shipboard machinery. One of the systems presented in the document was the Intelligent Control and Monitoring System (ICMOS).

The main functions of the ICMOS are performance monitoring, trend prediction, operational advice, and diagnosis. The system was capable of making performance checks for different loading and ambient conditions. Trending data and faults could be shown together with a prediction of future behavior of the monitored system. Operational advice would be provided

which, upon the occurrence of a fault, would indicate the time to criticality and indicate how to operate without causing damage. In the case of a deviation between actual healthy behavior is detected, a diagnosis would be performed. The diagnosis would indicate the cause of the malfunction and severity along with a confidence factor.

The ICMOS is based on a model of the engine realized in software. During operations, raw data from the sensors would be collected. Raw data would then be compared to the expected data from the model while simulating the actual operating conditions of the engine. After the raw data and model data has been compared, the resultant difference data is presented to the operator via the operator interface.

The interface provides the means by which the operator interacts with the system. Color displays provide the user with the capability to interrogate the system graphically and obtain information regarding the status of the system, components, and sensors. The interface is organized in a hierarchical organization of the engine and its components. At the top level there is a schematic representation of the engine in terms of its subsystems. Choosing any of the subsystems will result in the display of the schematic representation of the components and their connectivity together with the location of the sensors and their type. The color of the sensors, components and subsystems will change whenever there is a significant deviation from normal. In the event of a fault, the fault is presented to the operator along with the level of confidence. The operator has the option of accepting, deferring or rejecting the hypothesis. The operator can inspect and change the value of the sensor readings and have ICMOS reassess the diagnostic.

Problems

There seemed to be two basic problems. The first is how to detect a pending fault where the fault does not manifest itself until damage has occurred. The second is how to use this health or condition data once it has been collected. If the data is presented to the operator, he would soon be deluged with information. Hence, there must be a means by which the information is reduced to a point where it is useful to the human mind.

Wear on rotational machinery is a prime example where a fault has not manifested itself until damage has already been done. Typically, wear is detected by vibration analysis. However, the vibration fault signature does not appear until wear is sufficient enough to produce a measurable vibration. This points to the need for more instrumentation such as a temperature sensor.

Computer assistance is the obvious answer to the problem of the deluge of information presented to the operator. Software is available or can be developed which would perform the task of data reduction or integration. Mathematical models and heuristic knowledge can be realized in the software. However, there are a class of problems that cannot be solved mathematically or by rule-based reasoning. It is problems like this that neural networks offer significant promise.

It was stated that the data acquisition system needed a means by which to self check. Several instances were mentioned where a bad sensor would lead to a false alarm. This resulted in loss time. Another case that should be mentioned is overrating. Having tight specifications can result in excessive down time. Designing to more tolerant specifications could be a tool by which HM can increase reliability, decrease cost, and increase operational life.

Assessment

The document presented a program which yielded the very valuable first step lessons as to the approach. Prognostic research in the areas of trending and artificial intelligence is needed as the science of HM progresses. There are cases where whole subsystems can be monitored by monitoring the behavior rather than monitoring the internal components. The prime case is the diesel engine. In other cases such as bearings or fuel injectors, these components need to be monitored directly. These special components seem to be ones which require a higher level of maintenance. The area of the implementation has a foundation but the limitations are a function of the imagination of Systems Engineering.

Bearings are a case where condition or health monitoring will yield no fault indicating data until damage has occurred. Hence, heuristic methods would be an answer in that the expected life

of the bearing could be predicted. This means that perfectly good bearing might be replaced. But in either case, monitoring the health and well being of the bearing do not take into account such things as malalignment which would contribute to shorter life of the bearing.

When monitoring whole subsystems, such as the diesel engine, the condition or health of the subsystem can be closely monitored. Monitoring the intake air flow rate would indicate when maintenance should be performed such as the air filter needs to be cleaned or replaced. Blow-by pressure monitoring can indicate piston ring wear. Pattern recognition of acoustical sound would detect faulty valves or blown head gasket.

APPENDIX III 2

NEURAL NETWORK APPROACH TO SPACE SHUTTLE MAIN ENGINE HEALTH MONITORING

Approach

The approach was to select data from a test where a know anomaly did occur. Power spectra from a few hundred seconds of actual test data, where anomalies were known to occur, from NASA tests 901-364 and 904-044 were used to test the neural network. Test 901-364 contained an anomaly in the low-frequency temperature and pressure data and high-frequency strain gauge data in 904-044. Since data was presented to the neural network in discrete samples over a period of time called FFT window, the neural network must be able to identify the anomaly during the last FFT window prior to the emergency shut-down. In other words, the neural network must be able to identify an anomaly in sufficient time so that fault tolerant action or corrective action can be taken. The study was to investigate the capability of a neural network to identify an anomaly during the FFT window where the anomaly did occur.

Success

The investigation was a success as it indicates and demonstrates that neural networks can recognize anomalies during the sampling period of a FFT window. Further, the test shows that neural networks can be trained with fault free operational data. After training, the network can identify the deviation from normal operation. Given that the operational data collected by the sensors will change when a control action is implemented, it is possible for the network to tolerate the change in operational data along with the inherent background noise. If this line of progress, in this application science is continued, neural networks can be trained with normal operational data. This type of data is much easier and cheaper to collect. Having the sufficient training data available is one of the prerequisites for the effective application of neural networks to Health Management.

Problems

Normal operational data was used to train the networks. Failure data to train the neural networks is not readily available and hence was not used to train the network. Several cases of failure data from the same type sensor is needed to train the network if the network is to be able to recognize the failure. Because normal operational data was used to train the network, the network could only predict or identify an anomaly when there was a deviation from the expected normal. Hence, the network does not identify an anomaly, it identifies an unknown.

Assessment

Much work is needed before neural networks can be used effectively. Much study on the subject of neural networks is needed but the use of neural network shows a great deal of promise. Even though there is a great deal of evidence which indicates that neural networks is the answer, the science of the application of neural networks in real systems is not mature. In order to mature the science, neural networks should be used in cases where the benefits is realizable and beneficial. As research continues and lessons learned are generated, the application of neural networks will mature.

APPENDIX III 3

HEALTH MONITORING SYSTEM FOR THE SSME HARDWARE ARCHITECTURE STUDY

Approach

The major objective of the program, of which this paper was written, was to assess and evaluate candidate approaches for detecting SSME failures before the red-line cutoff. The approach included a study of fault detection algorithms, and an assessment of existing and near term sensor technologies. The fault detection approach, developed by UTRC, used algorithms and a system hierarchy which exploited the interrelated characteristics of the SSME components and parameter measurements.

The report is an architectural study for a SSME Health Monitoring System, with one of the requirements being that the design could be flown on the launch vehicle. However, the initial study would be done on the SSME test stand. It was accepted as a given that the test site system would not be flight worthy but would have more processing power since weight would not be a problem. In addition, the test sight would provide a test bed to validate and test the algorithms.

Problems

Since the program was a study, there were no real problems identified due to the application. However, there seemed to be three areas of concern, algorithms, throughput, and weight.

A set of three algorithmic approaches were developed and implemented to detect faults, observing gradual long term trends, detecting quick and high amplitude excursions, and observing oscillatory or non-steady state behavior. A sensor fusion technique was developed to detect failures which manifest themselves as gradual trends in performance parameter measurements and to distinguish this deviation from trends associated with normal engine operation. Autoregressive moving average models, based on time series analysis, were developed to detect fast excursions in engine parameters and also changes of engine parameters due to the transition of the engine from a stationary to a non-stationary condition. The Recursive Structural Identification (RESID)

algorithm was used to develop a regressive model between the SSME propellant flows and the thrust chamber pressure during open-loop start and shut-down.

In any real time system, throughput is always critical. Based on the throughput analysis, over 200 MIPS are required. The analysis also provides some insight into the complexity of the hardware. On the basis of throughput, there is expected to be no difference between the flight HMS and the ground system. In reality it is expected that the flight hardware would have less processing power because of weight restrictions.

Assessment

As stated in the conclusion, a design methodology was demonstrated which would provide for the transition of a Health Management system from the test stand to the flight vehicle. Since the ground based HMS system does use existing instrumentation, it is believed that the HMS system can be designed, developed, and fielded within five years.

APPENDIX IV

DEFINITIONS

1. Algorithm

A rule stated as a procedure for solving a problem. In the case of Health Management, it detects and isolates and recovers from functional problems, performs trend analysis and cross checks data. Four Types: Hard Limit

Relational Limit
Time Modified Limit
Logical Limit

2. Statement

Facts on a given condition which declare relationships to one or more other conditions. Used to define Intersystem Relationships which may, or may not, be suitable to be defined in an equation.

3. Software Logic

Coded information (Algorithms or Statements) used by a computer to detect, prevent, isolate, and/or recover from functional problems.

4. LRU

Line Replaceable Unit (An available Spare)

5. Redundant/Backup

A secondary Functional Element(s) (hardware or path) which performs the same purpose as the primary element. Maybe "like" or "unlike". Measurements with definable, related information are a form of redundancy and make the system fault tolerant.

6. Functional Failure/Fault

An unacceptable operation of an "active" Functional Element (a component or a group of components) which has been chosen to perform a specific purpose, or job, and to operate within defined parameter values and boundaries. "Functional Element" is usually depicted as a "Functional Block" in a "Functional Block Diagram".

7. **FF-DAREL**

(Functional Failure-Definition and Resulting Effects Listing). It identifies Functional Failures, Modes, Indicators and Effects

8. **Failure Mode**

Ways that a "Functional Element" can fail, i.e. "switch fails closed"

9. **Failure Effect**

The consequences that a Functional Failure can cause

10. **Time To Effect-Criticality**

The maximum time from occurrence of a Functional Failure until effects occur (Effects may, or may not, be reversible)

11. **DIP**

(Diagnostic Information Processing) Housekeeping and Control data generation, information gleaning, and automated fault prediction, detection, prevention, and recovery (Same as Integrated Diagnostic Concept)

12. **Integrated Diagnostic Concept**

Same as DIP

13. **Information**

Data communicated to a decision making process (human or machine) which contains a level of intelligence necessary to make those decisions.

14. **Probability of Mission Success**

The mathematical prediction (basis) for meeting criteria judging a mission to be successful, and given in the form of a ratio of successes to a total number of attempts.

15. **Aural Definition of Intersystem Relationships (ADIR)**

Brute force, manual, driving out Intersystem Relationships by direct discussions between skilled systems designers/engineers. The System Engineer, while participating in the discussions, compiles these definition/relationships from vocal designer inputs.

16. Aural Definition of Intersystem Relationships With Modeling Assistance (ADIRMA)

Defining of Intersystem Relationships (ADIR) supplemented by standard modeling techniques.

17. Aural Definition With ANN Modeling (ADAM)

Defining Intersystem Relationships (ADIR) supplemented by Artificial Neural Networks Projections

18. Availability

The operability of a system as a function of time. [A(t) is the probability that the system is operational at the instant of time, t]

19. Fault Containment/Fault Containment Region

Preventing a Functional Failure in a Functional Element from causing a Functional Failure in other Functional Elements.

20. Health Management

Those processes, techniques, and technologies used to define, design, analyze, build, verify, and operate a system from the viewpoint of preventing, or minimizing, the effects of failure or degradation. It supports all ground and flight elements during manufacturing, refurbishment, integration and operation through combined use of hardware, software, and personnel.

21. Proactive

A word formed by replacing the "Re" with "Pro". In Health Management, it means "Acting in anticipation of future problems, needs, or- changes."

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE Dec 15, 1995		3. REPORT TYPE AND DATES COVERED May 18 - Dec 15, 1995
4. TITLE AND SUBTITLE Generic Health Management A System Engineering Handbook Overview and Processes			5. FUNDING NUMBERS NAS8-40365	
6. AUTHOR(S) Lee Wilson, Jim Spruill, Yin Hong				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Alpha Technology 3322 S.Memorial Parkway, Suite 215-H Huntsville, AL 35801			8. PERFORMING ORGANIZATION REPORT NUMBER None	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Aeronautics & Space Administration Marshall Space Flight Center MSFC, AL 35812			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES Final Report Required by the Contract				
12a. DISTRIBUTION / AVAILABILITY STATEMENT			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) Health Management, a System Engineering Process, those processes-techniques-and-technologies used to define, design, analyze, build, verify, and operate a system from the viewpoint of preventing, or minimizing, the effects of failure or degradation.				
14. SUBJECT TERMS Health Management Follow-Up Study			15. NUMBER OF PAGES 74	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE None	19. SECURITY CLASSIFICATION OF ABSTRACT None	20. LIMITATION OF ABSTRACT	